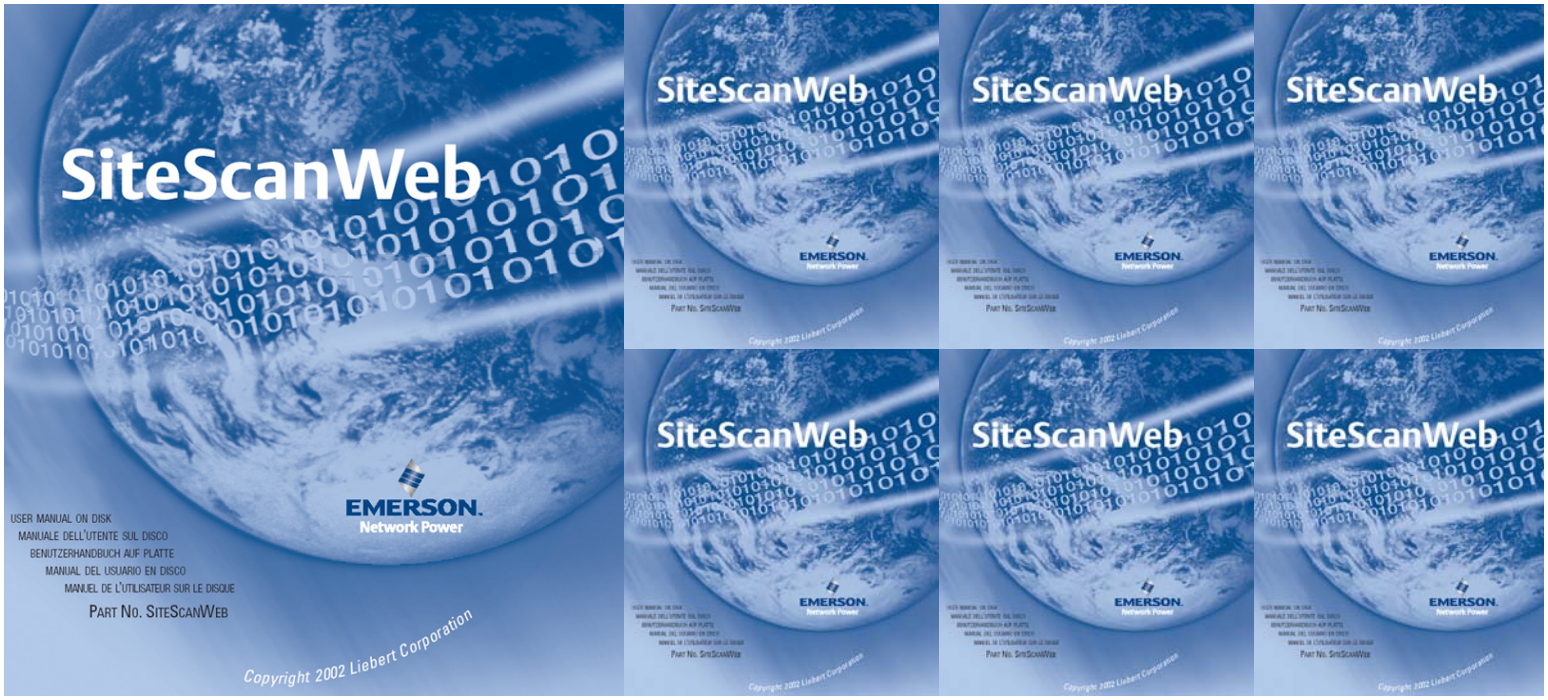
Site Monitoring and Services for Business Critical Continuity

SiteScan Web

Operation Manual



Liebert®

EMERSON™
Network Power

TABLE OF CONTENTS

SITESCAN WEB 1

1.0 WHAT IS SITESCAN WEB? 2

1.1 How Does SiteScan Web Work? 2

1.2 Purpose of This Manual 2

2.0 HOW DO YOU CONTACT LIEBERT FOR TECHNICAL SUPPORT? 3

3.0 WHO CAN BENEFIT FROM SITESCAN WEB? 4

3.1 Data Center 4

3.2 Facility 4

3.3 Enterprise 4

3.4 BMS Interface 4

4.0 WHAT IS REQUIRED TO USE SITESCAN WEB? 5

4.1 SiteScan Web Server Requirements 5

5.0 TYPICAL SITESCAN WEB SYSTEM 6

6.0 OVERVIEW OF SITESCAN WEB 7

6.1 The SiteScan Web Workspace 7

6.2 Menus and Buttons 8

6.3 Informational Icons in the Navigation Tree 9

6.4 SiteScan Web Features 10

7.0 GETTING STARTED WITH SITESCAN WEB 11

7.1 Start SiteScan Web 11

7.2 Log on 11

8.0 VIEWING STATUS 12

8.1 View Device Status 12

8.2 Choose a Different Graphic 13

9.0 MANAGING ALARMS 14
9.1 Alarms Window Overview 14
9.2 View Alarms 15
9.2.1 View the Alarm List 15
9.2.2 Acknowledge and Delete Alarms 16
9.3 Messages 17
9.4 Actions 18
9.4.1 Alarm Popup Action 19
9.4.2 Print Action 20
9.4.3 Run External Program Action 21
9.4.4 Send Alphanumeric Page Action 22
9.4.5 Send E-Mail Action 24
9.4.6 Send an SNMP Trap Action 25
9.4.7 Write Property Action 26
9.4.8 Write to Database Action 27
9.4.9 Write to File Action 29
9.4.10 Field Code Definitions 30
9.5 Enable/Disable 32
9.5.1 Enable or Disable Features 32
9.5.2 View Selected Sources 33
9.6 Alarm Reports 34
10.0 VIEWING TRENDS 35
10.1 View Trends 35
10.1.1 Tools for viewing trends 36
10.2 Configure Trends 37
10.3 Create a New Trend Graph 37
11.0 VIEWING REPORTS 38
11.1 View Reports 38
11.2 Set Up Report Options 39
11.3 Set Up a New Report 40
11.3.1 Create a New Report 40
11.3.2 Design the New Report 41
11.4 Description of SiteScan Web Reports 42

12.0 CONFIGURING SITESCAN WEB 43

12.1 My Settings 43

12.1.1 Settings 43

12.1.2 Contact info 44

12.2 System Settings 45

12.2.1 General 45

12.2.2 Daylight Saving 45

12.3 Set Up Users 46

12.3.1 Set Up Operators 46

12.3.2 Create Operator Groups 47

12.4 Assign Privileges to Users 48

12.4.1 Add a Privilege Set 48

12.5 Services 50

12.6 Trends Setup 51

12.6.1 Trends Display Setup 51

12.6.2 Trends Print Setup 52

12.7 Client Installs 53

13.0 LIEBERT SOFTWARE PROGRAM LICENSE AGREEMENT 54

FIGURES

Figure 1 Alarm icons 9

TABLES

Table 1 Minimum requirements - SiteScan Web server* and client workstations 5
Table 2 View buttons and menu options - summary 8
Table 3 Features available in SiteScan Web 10
Table 4 Field code definitions 30
Table 5 Tools for viewing trend graphs 36
Table 6 Available reports 38
Table 7 Description of available reports 42
Table 8 Privilege descriptions 49

SITESCAN WEB

User Manual
Liebert® Corporation

Liebert Corporation	Liebert Europe	Liebert Asia
1050 Dearborn Drive P.O. Box 29186 Columbus, Ohio 43229 **Sales** Phone: 1 800 877 9222 FAX: 1 614 841 6022 **Technical Support** Phone: 1 800 222 5877 FAX: 1 614 841 5471 E-mail: monitoring@liebert.com	Via Leonardo Da Vinci 8 Zona Industriale Tognana 35028 Piove Di Sacco (PD) Italy Phone: 39 049 9719 111 FAX: 39 049 5841 257	7/F, Dah Sing Financial Centre 108 Gloucester Road, Wanchai Hong Kong Phone: 852 25722201 FAX: 852 28029250
Liebert Web Site: http://www.liebert.com **SiteScan Web Web Site: http://sitescan.liebert.com**		

SL-27050 (February 10, 2006)

1.0 WHAT IS SITESCAN WEB?

SiteScan Web uses a network of microprocessor-based control modules to monitor and control Liebert air, power, UPS and other critical equipment.

SiteScan Web enables the user to monitor and control equipment in a single building, an entire campus or a network of facilities around the globe. A SiteScan Web system utilizes a Web-based server running Windows XP, 2003 Server or 2000 and a conventional Web browser to gather information, change operating parameters, run reports and perform similar functions on various types of critical equipment.

1.1 How Does SiteScan Web Work?

A central Web-based server communicates with control modules and generates Web pages that may be accessed using a conventional Web browser. SiteScan Web allows you to gather information, change operating parameters, run reports and perform other critical monitoring system functions on equipment in a single facility or in dozens of locations.

The Web server and Liebert gateway communicate over an Ethernet network. The Liebert gateway communicates to the Liebert control modules using the Control Module network (CMnet) and the ARCnet156 protocol. The control modules communicate with the Liebert environmental and power equipment using the Information Gathering Network (IGMnet) or to contact closure equipment using a signal cable.

Customers access the information presented as a result of these functions using a Web browser. Internet Explorer is the browser supported by the SSWEB server.

1.2 Purpose of This Manual

This manual is intended to serve as an operation manual for SiteScan Web. The manual presents instructions and illustrations to assist operators with day-to-day activities that may be required for managing a SiteScan Web system.

Functions typically performed by an LGS representative are not covered in this manual:

- Installing the SiteScan Web software
- Connecting equipment that will be monitored by SiteScan Web
- Configuring equipment in the SiteScan Web software

2.0 How Do You Contact Liebert for Technical Support?

For help on deciding how to set up SiteScan Web or any other Liebert monitoring product, contact Liebert's Software Technical Applications Support Center at:

UNITED STATES	Phone: 1 800 222 5877
FRANCE	Phone: +33 1 43600177
GERMANY	Phone: +49 89 9050070
ITALY	Phone: +39 049 9719111
NETHERLANDS	Phone: +31 33 2474074
UNITED KINGDOM	Phone: +44 1628403200
WORLDWIDE	Phone: 1 614 841 6755
	FAX: 1 614 841 5471
	All Products: **http://www.liebert.com** SiteScan Web: **http://sitescan.liebert.com**
	E-mail: **monitoring@liebert.com**

3.0 WHO CAN BENEFIT FROM SITESCAN WEB?

Any industry operating devices utilizing the BACnet protocol can benefit from using SiteScan Web to protect valuable equipment, data and other assets in the event of power or mechanical failure.

Different people in an organization need to know different things about the operation of critical facilities. SiteScan Web has the unique ability to be tailored to provide various levels of information to those in your organization responsible for system operations.

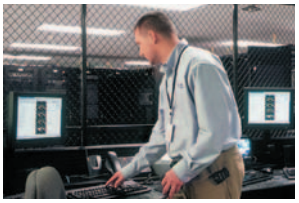
Examples include personnel running a data center, an entire facility, an enterprise-wide network or a building management system (BMS).

3.1 Data Center

Those responsible for the operation of large data or telecommunications centers must be aware of all protective infrastructure within these facilities.

They need up-to-the minute information that will allow them to keep systems operating—no matter what the situation.

3.2 Facility



These people are interested in the performance of critical operations in the context of an entire facility.

Events in one area of a facility can directly affect the operation of critical systems in another and vice versa.

3.3 Enterprise

Multiple sites mean multiple responsibilities for those in charge of an enterprise-wide network and communications system.

They need to know the status of many remote locations to keep the entire organization working smoothly.

3.4 BMS Interface

SiteScan Web can interface with an existing building management system (BMS) or other facility supervisory equipment for expanded monitoring capability.

4.0 WHAT IS REQUIRED TO USE SITESCAN WEB?

Visit the Liebert Web site at **http://sitescan.liebert.com** for the latest product information. The Web site always has the most detailed and up-to-date information on system requirements and SiteScan Web's capabilities.

4.1 SiteScan Web Server Requirements

SiteScan Web is based on server/thin-client architecture, designed around the open standards of Web technology. The SiteScan Web Server communicates using ASHRAE's BACnet/IP protocol and is accessed using a Web browser over the owner's intranet or external through the Internet. The intent of the thin-client architecture is to provide operators complete access to the system via a standard Web browser. The thin-client Web browser Graphical User Interface (GUI) supports Microsoft® Internet Explorer (version 5.5 or later). The SiteScan Web server software supports Windows 2000 and XP platforms and support for Windows 2003 Server.

System configuration requirements differ slightly for the SiteScan Web server and any associated client workstations. **Table 1** shows the recommended requirements for the server and client workstations running on a Microsoft Windows Platform.

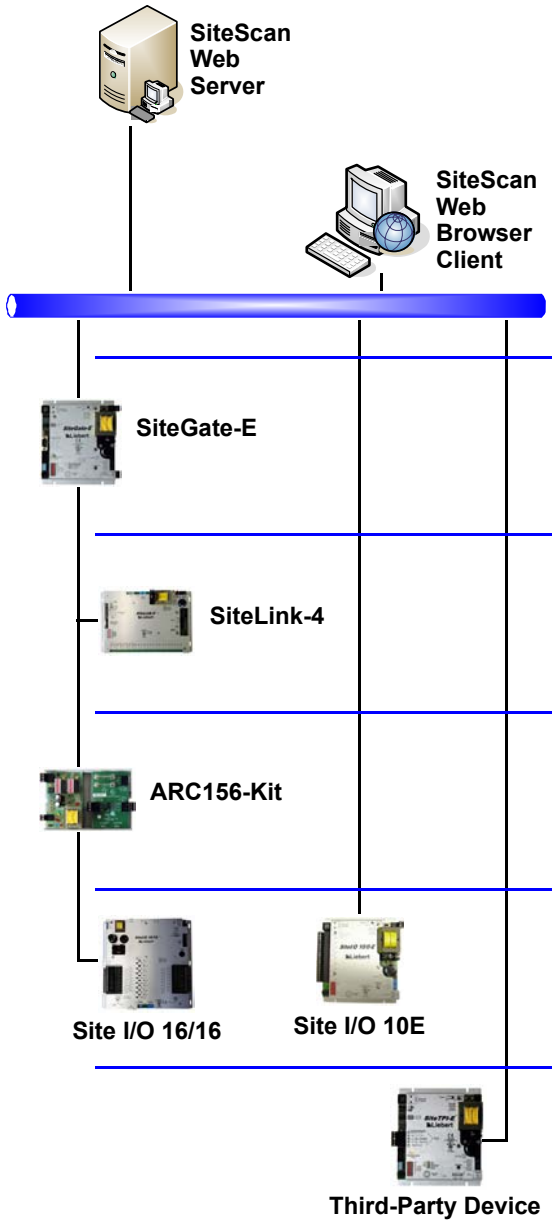
Table 1 Minimum requirements - SiteScan Web server* and client workstations

Feature	Minimum Server Requirements*	Client Workstation Requirements
Operating system	Windows 2000, 2003 or XP	Windows 95, 98, NT 4.0, 2000, XP
Browser	Microsoft Internet Explorer v5.5 or later with Sun Systems Java (**www.java.com**)	Microsoft Internet Explorer v5.5 or later with Sun Systems Java (**www.java.com**)
Computer system (CPU) speed	The more simultaneous users on a system, the faster the CPU speed required to maintain good user response time. For a system with: • One or two active users, a 2 GHz CPU should provide adequate performance. • Three or more active users, select a 3 GHz or faster CPU. • 10 or more active users, consider multiple CPUs. Moving the database to another computer is more economical than running both SiteScan Web and the database on a multiple CPU system.	For adequate performance under Windows 95, 98 or NT 4.0: • 700 MHz Pentium® III processor with 512Mb RAM. For adequate performance under Windows 2000 or XP: • A processor of 1.5Ghz or better is recommended.
System memory	1024Mb system memory recommended to eliminate excessive swap file usage. The responsiveness of larger systems will benefit directly from more memory.	—
Hard disk space	2Gig free hard disk space available for SiteScan Web **Note:** A SCSI hard disk interface is recommended for users making extensive use of alarms or historical trends.	10Mb of free hard disk space available for caching images
USB ports	USB ports available for system backups, preferably front-mounted to avoid disturbing computer room cabling.	—
CD drives	CD-ROM drive (CD-RW drive recommended for alternate backup purposes)	—
Mouse/ keyboard	2-button mouse / 104-key keyboard	2-button mouse / 104-key keyboard
Remote control software	For large systems with remote sites, Liebert strongly recommends using remote control software—for example, Windows Remote Desktop, VNC or PC Anywhere—to allow Liebert service engineers to access the server remotely.	—
Display	SVGA display card and monitor that support a resolution of 1024x768 pixels with True Color (32-bit) or better	SVGA display card and monitor that support a resolution of 1024x768 pixels with High Color (16-bit) or better
Network	10/100 Mbps Ethernet network card	Network connection capable of reaching the server—for example, an Ethernet network card or a dial-up modem connection.

* SiteScan Web should have its own dedicated server. Having other web server applications—such as Apache or IIS—running on the same machine will cause conflicts.
Running the client-side browser on the server will add to the the server's load; to compensate, increase CPU and memory headroom.

5.0 TYPICAL SITESCAN WEB SYSTEM

A typical SiteScan Web system may include the components shown in the figure below.



Server Software and Client License

- **SiteScan Web Server** - A dedicated computer running SiteScan Web server software, including a database that stores system configuration, custom graphics and equipment interfaces. For hardware and operating requirements, see **Table 1**.
- **SiteScan Web Client** - A workstation on the network that uses a conventional Web browser, such as Internet Explorer, to access the SiteScan Web server. The workstation may also be used for functions not related to SiteScan Web.
- **Ethernet Backbone** - The customer's existing network, including router and wiring or wireless connection gear.

Router Gateway

- **Ethernet Gateway** - The gateway that communicates with the SSWEB server, other Ethernet gateways and the control module network.

IGM Interface Control Modules

- **SiteLinks** - Control modules that provide IGM communications between the Liebert environmental and power equipment and the Liebert gateway.

ARCnet Communication Devices

- **ARCnet devices** - An ARC156-Kit, which must be installed on every ARC156 network; controls biasing and proper termination of the ARC156 network.

Input/Output Control Modules

- **Site I/O Modules** - A selection of modules that translate analog and digital signals within your critical environments. These modules may provide digital signals for output control.

Third-Party Interfaces

- **SiteTPI-E** - A monitoring and control module that enables non-Liebert Modbus devices to be incorporated into the SiteScan Web System; used to interface with third-party equipment such as generators, fire suppression systems or competitive gear.

6.0 Overview of SiteScan Web

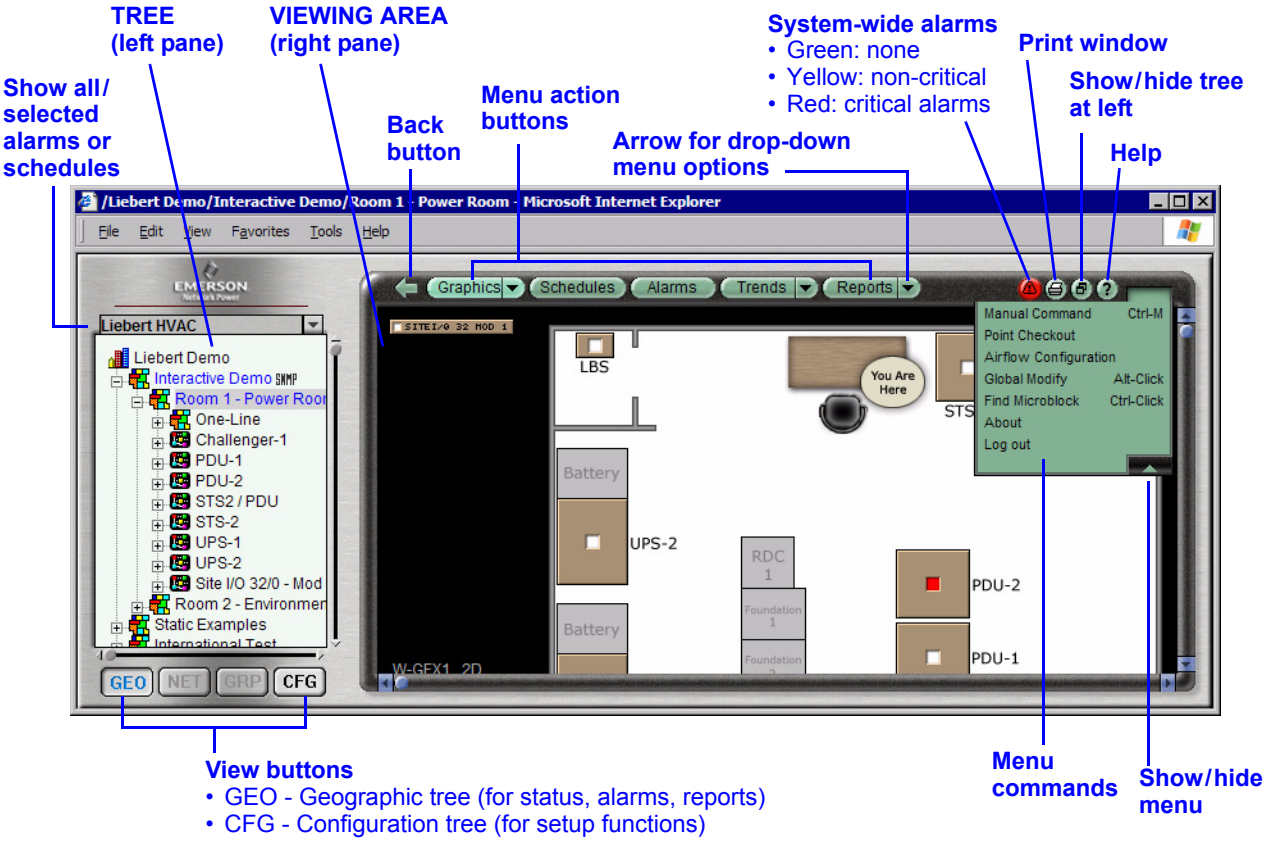
This section provides a quick look at the navigation and configuration features available through SiteScan Web's buttons and tabs.

SiteScan Web's view buttons—GEO and CFG—logically divide SiteScan Web's functionality.

- The **GEO** button displays the operational status and condition of configured devices.
- The **CFG** button is the entry point for all setup functions.

6.1 The SiteScan Web Workspace

The main parts of the SiteScan Web window are shown in the following example.



6.2 Menus and Buttons

Table 2 shows the main SiteScan Web features discussed in this manual and where to learn more about each.

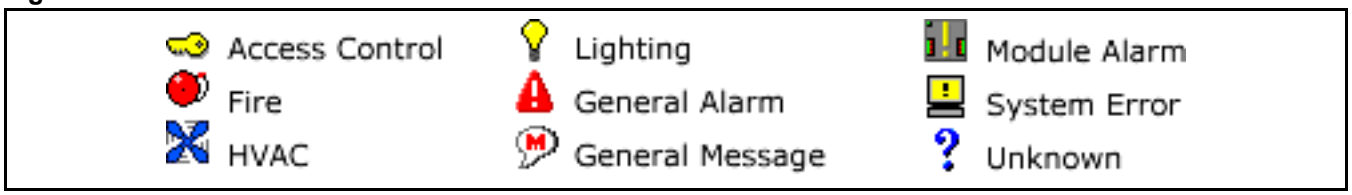
Table 2 View buttons and menu options - summary

Feature	Tab	Subcategories	For more information, see:
GEO View Button			
Graphics	—	—	**8.0 - Viewing Status**
Alarms	View	—	**9.2 - View Alarms**
	Messages	—	**9.3 - Messages**
	Actions	Alarm Popup	**9.4.1 - Alarm Popup Action**
		Print	**9.4.2 - Print Action**
		Run External Program	**9.4.3 - Run External Program Action**
		Send Alphanumeric Page	**9.4.4 - Send Alphanumeric Page Action**
		Send E-Mail	**9.4.5 - Send E-Mail Action**
		Send SNMP Trap	**9.4.6 - Send an SNMP Trap Action**
		Write Property	**9.4.7 - Write Property Action**
		Write to Database	**9.4.8 - Write to Database Action**
		Write to File	**9.4.9 - Write to File Action**
	Enable/Disable	—	**9.5 - Enable/Disable**
	Reports	—	**9.6 - Alarm Reports**
Trends	View	—	**10.1 - View Trends**
	Configure	—	**10.2 - Configure Trends**
Reports	View	—	**11.1 - View Reports**
	Configure	—	**11.2 - Set Up Report Options**
	Design	—	**11.3 - Set Up a New Report**
CFG View Button			
My Settings	Settings	—	**12.1.1 - Settings**
	Contact Info	—	**12.1.2 - Contact info**
System Settings	General	—	**12.2.1 - General**
	Daylight Saving	—	**12.2.2 - Daylight Saving**
Operators	—	—	**12.3.1 - Set Up Operators**
Privilege Sets	—	—	**12.4.1 - Add a Privilege Set**
Operator Groups	—	—	**12.3.2 - Create Operator Groups**
Services	—	—	**12.5 - Services**
Trends Display Setup	—	—	**12.6.1 - Trends Display Setup**
Trends Print Setup	—	—	**12.6.2 - Trends Print Setup**

6.3 Informational Icons in the Navigation Tree

The alarm icons used in the navigation tree are shown in **Figure 1**.

Figure 1 Alarm icons



The icon indicates the alarm category. The icon's color indicates severity, as shown below:

Color	Severity
Blue	Maintenance needed
Yellow	General non-critical alarm
Red	Critical alarm

6.4 SiteScan Web Features

Table 3 lists the features available in SiteScan Web.

Table 3 Features available in SiteScan Web

	SiteScan Web	SiteScan 2000 w/ Alert
System Feature		
Current Version	3.0	2.6 w/ 3.0
Operating Systems	Windows NT 4.0 w/SP6 or higher, Windows 2000, Windows XP, Windows 2003 Server	Windows 95, Windows 98 & Windows ME
Internationalization	English, Spanish, French, Dutch, Germany & Simplified Chinese, Traditional Chinese, Korean	
Database	MS Access, SQL Server & Oracle	
Server-Based	Internet Explorer	Client Software Required
Help	HTML Based	Windows Help
Security		
User Privileges & Accounts	✔	
Run as Service	✔	
Automatic Logout	✔	✔
Operator Audit Logging	✔	✔
Graphics		
3-D Floorplans	✔	✔
2-D Floorplans	✔	✔
Trending	✔	✔
Trend Historian	✔	✔
Alarm Management		
Alarm Filtering	✔	✔
Multiple Alarm Management	✔	✔
Comments to Alarm	✔	✔
Change Colors of Alarms		✔
Reporting Actions		
Alarm Escalation		✔
ASCII File Write	✔	✔
Numeric Paging		✔
Alpha-Numeric Paging	SMTP	Modem Dial-Out (TAP Only)
Parallel Print	✔	✔
Serial Output	✔	✔
Play Sound Wave	✔	✔
Run External Command	✔	✔
Facsimile		✔
Email	✔	w/SiteTrap
LGS Remote Monitoring	w/Liebert RM Agent	P
SNMP	w/ Liebert RM Agent	w/ SiteTrap
Format the Output	✔	✔
Local Notifications		
Applications to Foreground		✔
Flash Application Icon		✔
Play Default Beep	✔	✔

7.0 GETTING STARTED WITH SITESCAN WEB

This section explains how to start the SiteScan Web application, log in and change your password. You should change the default password for security purposes.

Saving Changes

You must save certain changes to SiteScan Web. Whenever you make a change that is not yet saved, the Accept and Cancel buttons

appear at the top of the toolbar:

- Click on the **Accept** button

to save your changes.

or

- Click on the **Cancel** button

to cancel your changes.

Using Internet Explorer

SiteScan Web is designed to work in Microsoft® Internet Explorer. If you use a different browser, screens appear in Wireless Access Protocol (WAP) formats.

7.1 Start SiteScan Web

To begin a session:

- Click on the **Start** button, then on **Programs**, then on **Internet Explorer**.
- Type the address of the SiteScan Web server in the Address Bar and press the Enter key.

7.2 Log on

After connecting to the server, the login screen appears, as shown at right.

To log on:

- Enter the user name in the Name box.
- In the Password box, enter the password provided by LGS. To change the password, see **12.1.1 - Settings**.
- Click the **Log In** button.

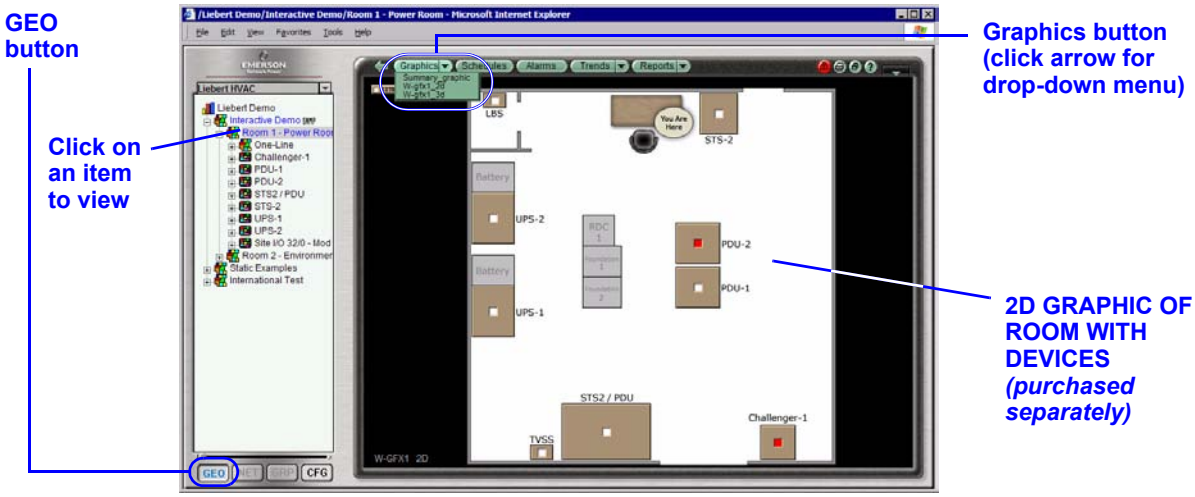
8.0 VIEWING STATUS

The **Graphics** button offers a quick look of the status of your entire system or any portion of it.

8.1 View Device Status

To view a graphic representation of your system:

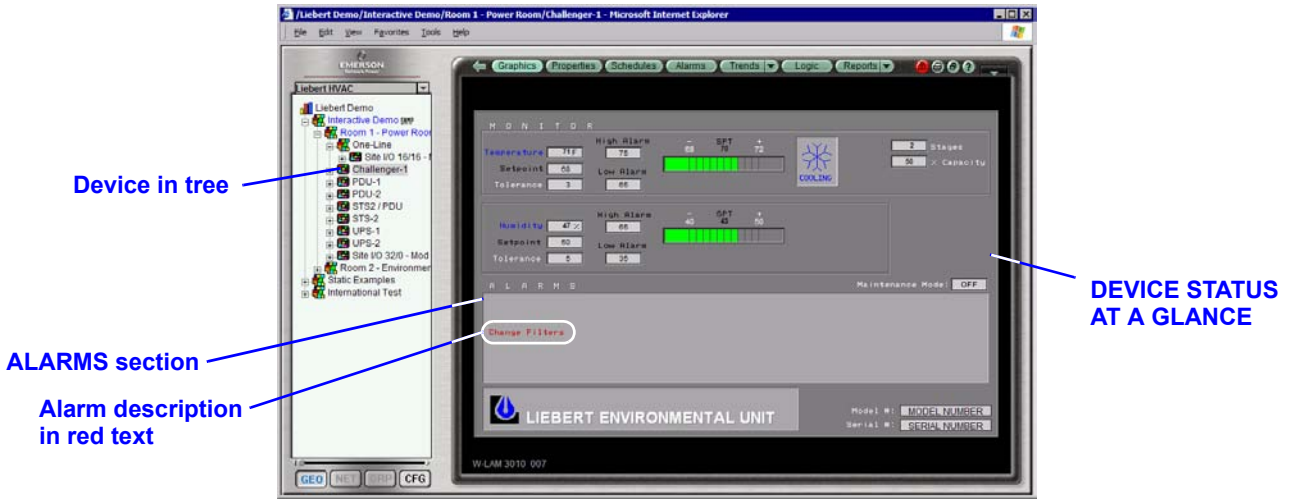
- Click the **GEO** button in the bottom left corner.
- Click on the item you want to view in the geographic tree at left—**Room 1 Power Room** in the example below.
- Click the **Graphics** menu action button at the top. The example below shows a 2D graphic in the viewing area. To display another type of graphic, see **8.2 - Choose a Different Graphic**.


GEO button
Click on an item to view
Graphics button (click arrow for drop-down menu)
2D GRAPHIC OF ROOM WITH DEVICES (purchased separately)

- If the displayed item has devices—a room with equipment, as in the example above—each device is color-coded to indicate whether any current alarms are present (red) or not (white), as shown below. For details on alarms, see **9.0 - Managing Alarms**.

Color	Indicates:
Red	A critical alarm is present
White	No alarms are present

- To view the status of an individual device at a glance, click on the device in the room graphic to display detailed information, as in this example of a Liebert environmental unit. Another way to view this device status window is by clicking on the item in the tree at left.



- In this type of device status window, the Alarms section displays descriptive text in red if the device has any current alarms, as in the example above, or “No Alarms Present” in green text.

8.2 Choose a Different Graphic

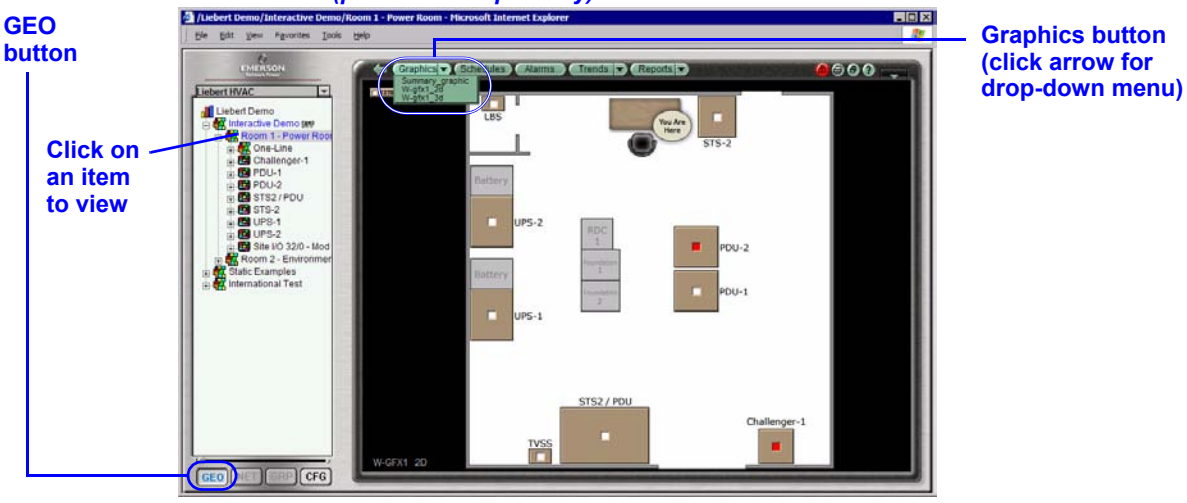
Three types of graphics are available in SiteScan Web:

- **2D Graphic** - a two-dimensional drawing of devices and placement (purchased separately)
- **3D Graphic** - a three-dimensional drawing of devices and placement (purchased separately)
- **Summary Graphic** - a text listing of all devices (standard)

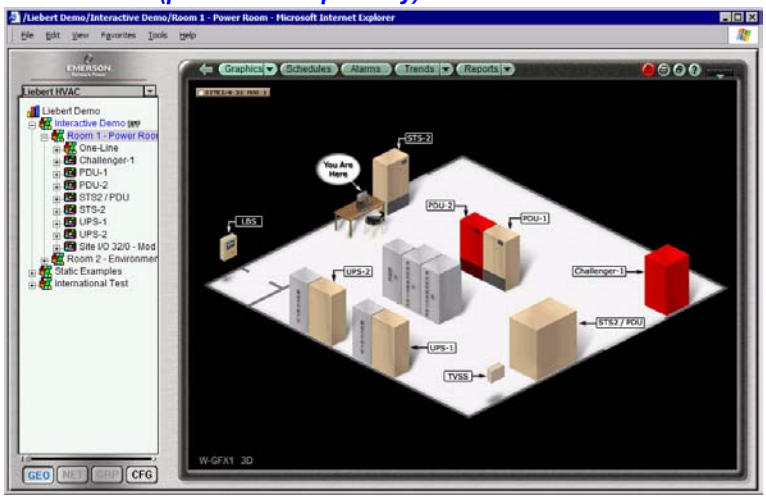
To choose a different graphic:

- Click the **GEO** button at bottom left, then click on the item you want to view in the tree at left.
- Click the down arrow on the **Graphics** button at the top, then choose the desired graphic from the drop-down menu.

2D GRAPHIC *(purchased separately)*



3D GRAPHIC *(purchased separately)*



SUMMARY GRAPHIC *(standard)*

9.0 MANAGING ALARMS

The **Alarms** button offers quick access to alarm-related features:

- View, acknowledge and delete alarms
- Set up actions that SiteScan Web performs when an alarm is received
- Customize alarms by changing the message
- Generate alarm reports to view, print or save to a file

9.1 Alarms Window Overview

- Click the **GEO** button in the bottom left corner.
- Click on an item in the tree at left—**Room 1 Power Room** in the example below.
- Click the **Alarms** menu action button at the top.
- The Alarms window has several tabs across the top; the example below shows the **View** tab.

GEO button
Click on an item to view
Alarms button (click arrow for drop-down menu)
/Liebert Demo/Interactive Demo/Room 1 - Power Room - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Graphics Schedules Alarms Trends Reports
View Messages Actions Enable / Disable Category Template Reports Room 1 - Power Room
Liebert HVAC
Liebert Demo
Interactive Demo
Room 1 - Power Room
One-Line
Challenger-1
PDU-1
PDU-2
STS2 / PDU
STS-2
UPS-1
UPS-2
Site I/O 32/0 - Mod
Room 2 - Environmer
Static Examples
International Test
GEO NET GRP CFG
1. Select one or more categories.
Select all:
View By: Date
Need Rtn Need Ack Closed
Here 35 3 95
Total 60 1521 132
Occurred To Do Alarm Report
Access Control Maintenanc
Fire System Critical
General Alarm
Liebert HVAC
Liebert Power
Liebert UPS
System Info
Unknown
01/19/2006 02:57:06PM CB2 S2 Open has returned to normal.
CB2 S2 Open at STS-2
01/19/2006 02:57:19PM Ouput Breaker CB3A Open has returned to normal.
Ouput Breaker CB3A Open at STS-2
01/19/2006 02:58:17PM Battery Fuse Fail has returned to normal.
Battery Fuse Fail at UPS-1
01/19/2006 03:01:06PM Change Filters alarm.
Change Filters at Challenger-1
01/19/2006 04:12:30PM Change Filters has returned to normal.
Change Filters at Challenger-1
Acknowledge Force Normal Delete Additional Actions

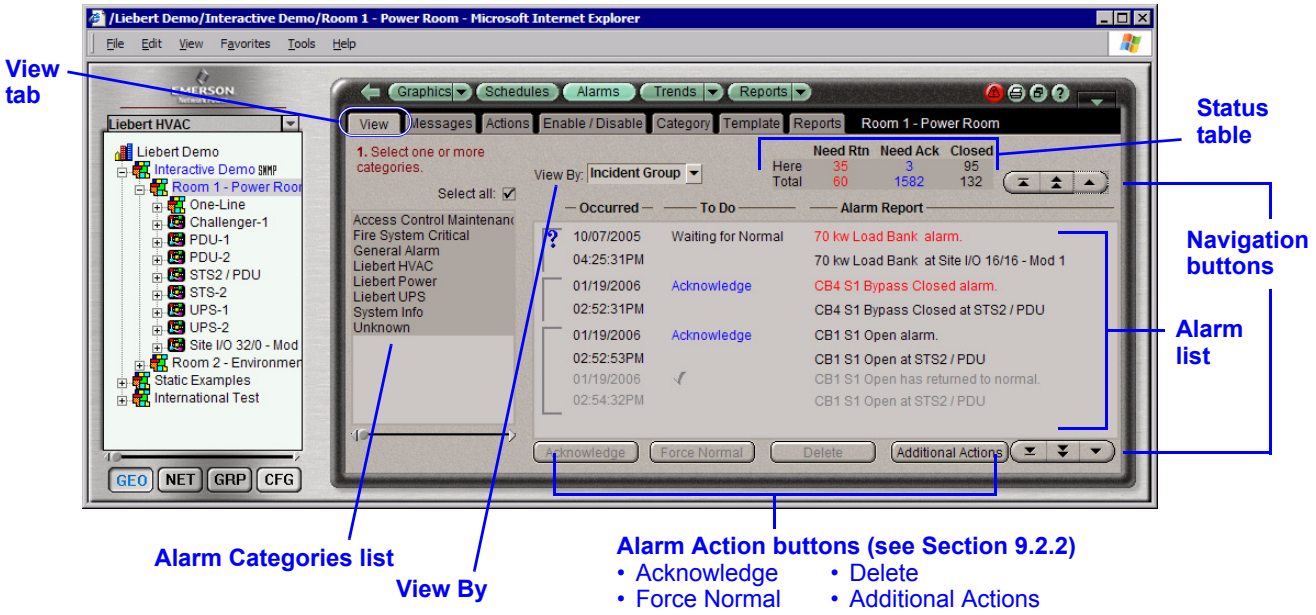
- The alarm list displays all alarms for the location selected in the tree at left, including all items below it in the tree.
- For details on viewing alarms, see **9.2.1 - View the Alarm List**.
- For instructions on responding to alarms, see **9.2.2 - Acknowledge and Delete Alarms**.

9.2 View Alarms

The **View** tab allows you to view alarms and perform functions such as acknowledging alarms.

To access the View functions:

- Click the **GEO** button, then click on an item in the tree at left.
- Click the **Alarms** button, then the **View** tab.


/Liebert Demo/Interactive Demo/Room 1 - Power Room - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Graphics Schedules Alarms Trends Reports
View Messages Actions Enable / Disable Category Template Reports Room 1 - Power Room
Liebert HVAC
Liebert Demo
Interactive Demo SNMP
Room 1 - Power Roo
One-Line
Challenger-1
PDU-1
PDU-2
STS2 / PDU
STS-2
UPS-1
UPS-2
Site I/O 32/0 - Mod
Room 2 - Environmer
Static Examples
International Test
GEO NET GRP CFG
1. Select one or more categories.
Select all:
Access Control Maintenanc
Fire System Critical
General Alarm
Liebert HVAC
Liebert Power
Liebert UPS
System Info
Unknown
View By: Incident Group
Need Rtn Need Ack Closed
Here 35 3 95
Total 60 1582 132
Occurred To Do Alarm Report
10/07/2005 04:25:31PM Waiting for Normal 70 kw Load Bank alarm.
70 kw Load Bank at Site I/O 16/16 - Mod 1
01/19/2006 02:52:31PM Acknowledge CB4 S1 Bypass Closed alarm.
CB4 S1 Bypass Closed at STS2 / PDU
01/19/2006 02:52:53PM Acknowledge CB1 S1 Open alarm.
CB1 S1 Open at STS2 / PDU
01/19/2006 02:54:32PM CB1 S1 Open has returned to normal.
CB1 S1 Open at STS2 / PDU
Acknowledge Force Normal Delete Additional Actions
View tab
Status table
Navigation buttons
Alarm list
Alarm Categories list
View By
Alarm Action buttons (see Section 9.2.2)
• Acknowledge
• Force Normal
• Delete
• Additional Actions

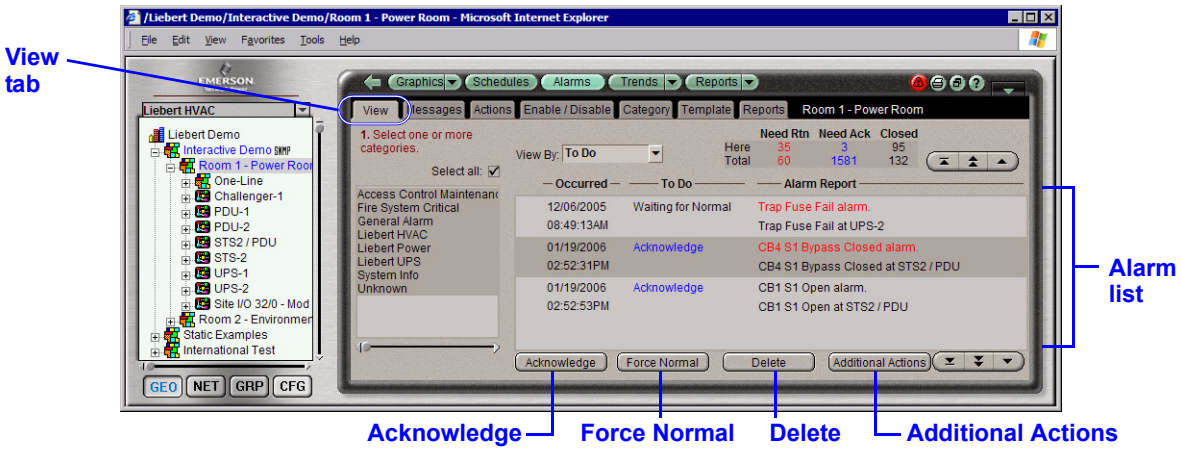
9.2.1 View the Alarm List

- Double-click on an alarm in the list to reveal or hide more details about the alarm. The alarm list displays three columns of information about each alarm:
  - **Occurred** The date and time the alarm was generated.
  - **ToDo** • **Acknowledge** indicates the alarm needs to be acknowledged.
    • **Waiting for Normal** indicates the alarm requires a return-to-normal.
    • A check mark (✔) indicates the alarm is closed.
  - **Alarm Report** Displays the alarm message—a text description of what occurred and where.
- Use the navigation buttons at right to scroll through the list one alarm at a time, a page at a time or to the beginning or end of the list.
- To view all types of alarms or choose from the Alarm Categories list:
  - To display all alarms, click to place a check mark (✔) in the Select All box.
  - To display only selected alarms, click on an item in the Alarm Categories list. (Control-click to select additional items.)
- To sort or filter the list, click on the down arrow to the right of the View By box, then select an option from the drop-down menu:
  - **Date** Displays all alarms sorted by the time each alarm was generated, from newest to oldest.
  - **To Do** Displays only alarms requiring one or more actions to be done before they can be closed.
  - **Incident Group** Groups all alarms related to a particular incident with a bracket to the left of the icons—for example, an alarm and its subsequent return-to-normal event form an incident group.
- The status table to the right of the View By box offers a quick glance at the current state of alarms at the location selected in the tree (**Here**) and in the entire system (**Total**):
  - **Need Rtn** Number of alarms that need a return-to-normal
  - **Need Ack** Number of alarms that need to be acknowledged
  - **Closed** Number of alarms that are closed

9.2.2 Acknowledge and Delete Alarms

To access the alarm action functions:

- Click the **GEO** button, then click on an item in the tree at left.
- Click the **Alarms** button, then the **View** tab.



Acknowledge a Single Alarm

- Select an alarm that shows *Acknowledge* in the ToDo column.
- Click the **Acknowledge** button below the list. A check mark (✔) appears in the ToDo column.

Force a Return-To-Normal State

If an alarm is not followed by a return-to-normal event, you can force a Return-To-Normal state:

- Select an alarm that shows *Waiting for normal* in the ToDo column.
- Click the **Force Normal** button below the list. A check mark (✔) appears in the ToDo column.

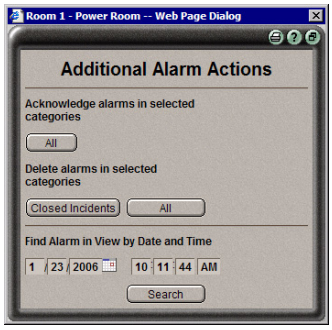
Delete a Single Alarm

- Select the alarm you want to delete from the list.
- Click the **Delete** button below the list. The alarm disappears from the list.

Additional Actions: Acknowledge or Delete Multiple Alarms, Search for an Alarm

The **Additional Actions** button allows you to acknowledge or delete multiple alarms all at once.

- Unless you want to acknowledge or delete all alarms, select the appropriate alarms—for example, click on View By **ToDo**, then highlight alarms that show *Acknowledge* in the ToDo column.
- Click the **Additional Actions** button below the list. The Additional Alarm Actions window opens, as shown at right.



Acknowledge Multiple Alarms

- To acknowledge multiple alarms, click the **All** button under Acknowledge Alarms in Selected Categories.

Delete Multiple Alarms

- To delete multiple alarms, click the appropriate button under Delete Alarms in Selected Categories:
  - **Closed Incident** Removes incident groups of related alarms in which all alarms have been closed.
  - **All** Removes all alarms at the selected location in the tree.
  - **All Systems** Removes all alarms in the entire system.

Search for an Alarm

- In this window, you may also search for an alarm generated on a particular date and time. Enter the desired date and time, then click the **Search** button. The Events screen will display the listing of alarm events as defined by the search criteria.

9.3 Messages

An alarm message is the text displayed in the Alarms **View** tab window and in alarm reports. An alarm message may consist of three parts:

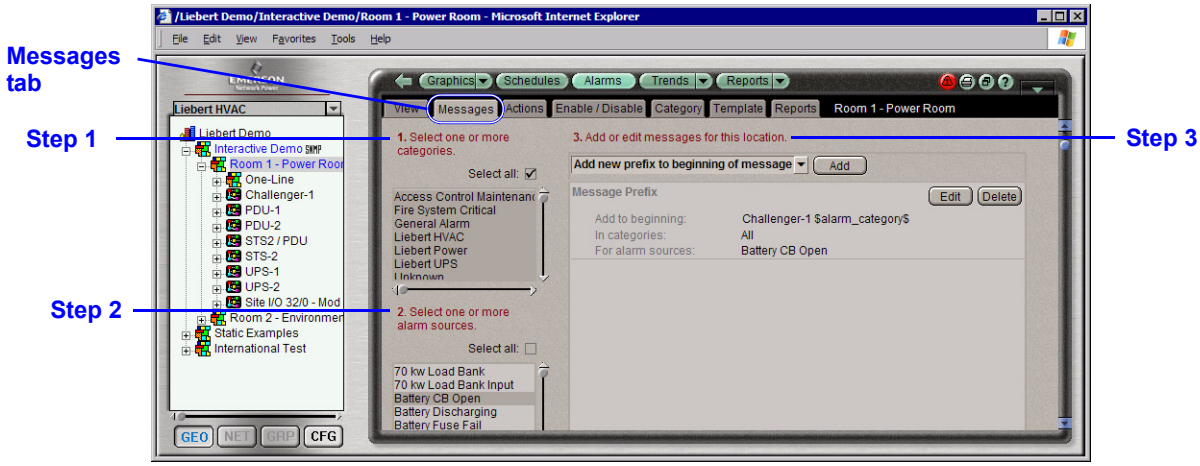
Prefix (optional)	Text	Details (optional)
Text at beginning of message	The alarm or return-to-normal	Text at end of message

This section describes how to add, change or delete the Prefix and Details portions of alarm messages.

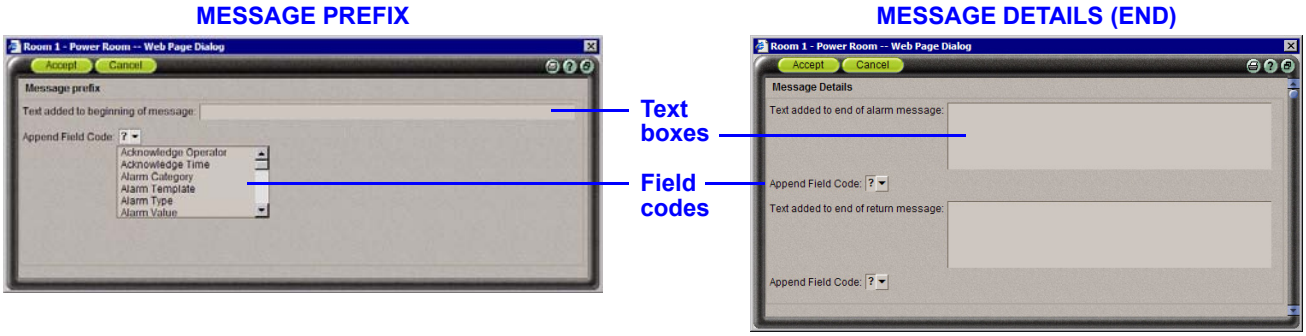
Changes apply to the location in the tree where they are added and to all its subordinate members of the tree. For example, if you add Details at the system level to show the Acknowledge Time for alarms in a certain category, that will appear in all alarm message for any element in the system.

To access the Message functions:

- Click the **GEO** button, then click on an item in the tree at left.
- Click the **Alarms** button, then the **Messages** tab. Steps are listed in red, as shown below.



1. Select the categories that contain the alarm sources whose messages you want to edit.
2. Select the alarm sources for the selected categories.
   Note: In **Steps 1** and **2**, control-click to select multiple items, or click the Select All check box.
3. Click on the down arrow and select an option from the drop-down menu: **Add new prefix to beginning of message** or **Add new details to end of message**.



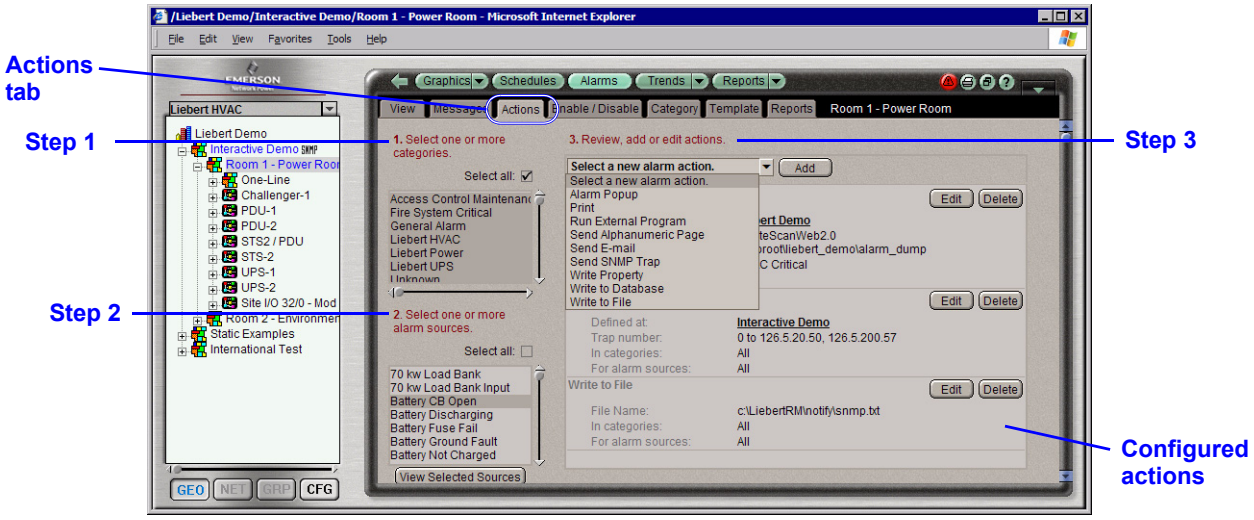
4. Click the **Add** button to open the appropriate window. The Message Details window, shown above right, allows you to make separate entries for alarms and return-to-normal events.
   - Type the text you want to add to the message in the text boxes.
   - To add a field code to a message, click the Append Field Code down arrow and select an option from the drop-down menu (see **Table 4** for definitions).
   - Click the **Accept** button to save your changes (or click **Cancel** to close without saving).
5. The new Prefix or Details appears in the **Messages** tab window. Click the **Edit** button to make additional changes. Click **Delete** to remove the item.

9.4 Actions

Certain SiteScan Web features may be set up to protect valuable equipment, data and other assets by responding automatically to alarms in devices affected by such events as power failures, overheating and mechanical failures.

For example, if a cooling unit's performance becomes impaired, SiteScan Web may be set up to send e-mail alerts to various personnel, record data pertaining to the event and append it to a particular file and launch a command or batch file that can execute user-customized scripts.

- Click the **GEO** button, then click on an item in the tree at left.
- Click the **Alarms** button, then the **Actions** tab. Steps are listed in red, as shown below.



1. Select the categories that contain the alarm sources you want to set up.
2. Select the alarm sources for the selected categories.
   Note: In **Steps 1** and **2**, control-click to select multiple items, or click the Select All check box.
3. To choose an action, click on the down arrow and select an option from the drop-down menu.
4. Click the **Add** button.
5. Proceed to the appropriate section to continue setting up the action.
   - **9.4.1 - Alarm Popup Action**
   - **9.4.2 - Print Action**
   - **9.4.3 - Run External Program Action**
   - **9.4.4 - Send Alphanumeric Page Action**
   - **9.4.5 - Send E-Mail Action**
   - **9.4.6 - Send an SNMP Trap Action**
   - **9.4.7 - Write Property Action**
   - **9.4.8 - Write to Database Action**
   - **9.4.9 - Write to File Action**

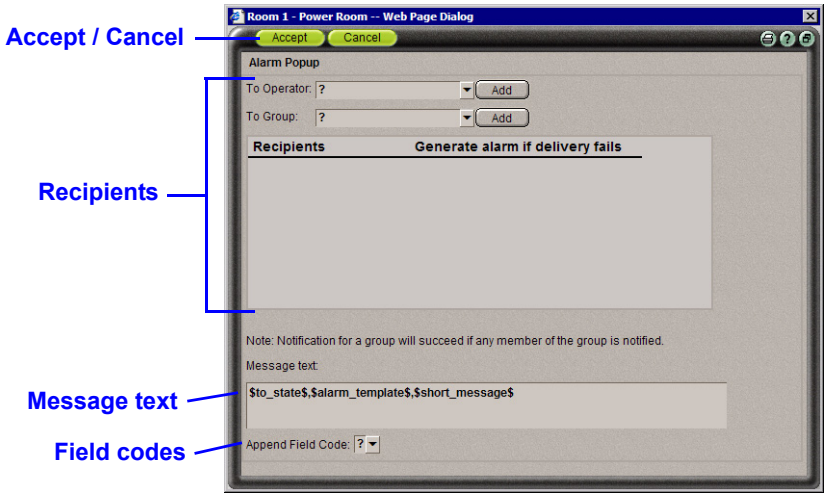
9.4.1 Alarm Popup Action

The Alarm Popup action sends an alert to designated recipients' computers when specified alarms occur. The alert pops up in a dialog box on each recipient's computer when an alarm occurs.

A recipient may be any networked computer running the SiteScan Web Alarm Popup application. Individuals and groups may be selected from a list set up via the CFG functions. For details on editing these lists, see **12.3.1 - Set Up Operators** and **12.3.2 - Create Operator Groups**.

Open the Alarm Popup window, shown below, to set up this action. To do this:

- Click the **GEO** button, then click on an item in the tree at left. When configured, the action will apply to the designated item in the tree as well as its subordinate items.
- Click the **Alarms** button, then the **Actions** tab.
- Select the alarm categories (**Step 1** in the **Actions** tab window) and alarm sources (**Step 2**) you want linked this action.
- Click on the down arrow (**Step 3**), select **Alarm Popup** from the drop-down menu and click **Add**.



- Specify the recipients who should receive notifications by clicking on the appropriate down arrow and selecting a name from the drop-down list:
  - Select an individual from the **To Operator** list, then click the **Add** button.
  - Select a group of operators from the **To Group** list, then click the **Add** button.
- Once added, the selected names appear in the Recipients list with a check box in the **Generate Alarm if Delivery Fails** column. Click to place a check mark (✔) to send a System Info alarm to the SiteScan Web server if the recipient is not running the Alarm Popup application when an alert is sent.
- In the Message Text box, enter the message as you want it to appear in the popup window, using the appropriate punctuation, including spaces and returns to separate lines of text.
- You can add dynamic alarm data to the text by selecting field codes from the Append Field Code list (see **Table 4** for definitions). To do this:
  - Place the cursor in the Message Text box where you want the data to appear.
  - Click on the Append Field Code down arrow, then select an option from the drop-down list.
- When finished, click the **Accept** button (or **Cancel** to close the window without saving your changes).

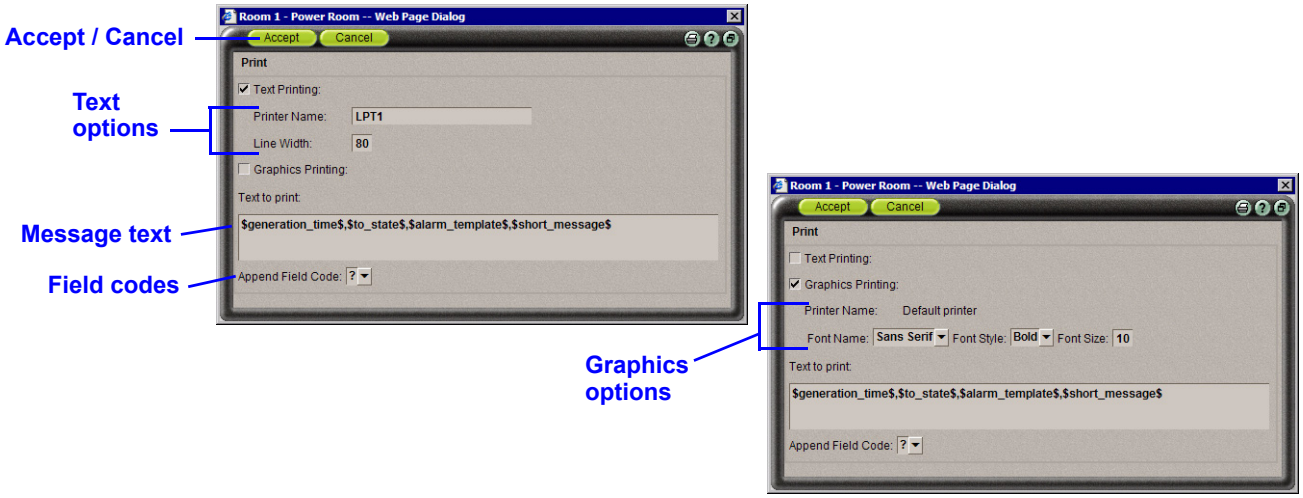
Once the action is set up, it appears in the **Actions** tab window. You may click the **Edit** button to make changes or the **Delete** button to remove it.

9.4.2 Print Action

The Print action sends an alert to a designated printer when a specified alarm occurs. The printed message may be sent to any printer connected to the server or a workstation on the network.

Open the Print window, shown below, to set up this action. To do this:

- Click the **GEO** button, then click on an item in the tree at left. When configured, the action will apply to the designated item in the tree as well as to its subordinate items.
- Click the **Alarms** button, then the **Actions** tab.
- Select the alarm categories (**Step 1** in the **Actions** tab window) and alarm sources (**Step 2**) you want linked this action.
- Click on the down arrow (**Step 3**), select **Print** from the drop-down menu and click **Add**.



- Click to place a check mark (✔) to choose a printing method based on the printer type:
  - Select **Text Printing** when using a dot matrix printer; this prints multiple alarms per page.
    Enter the designated name of the printer in the Printer Name box—for example, **LPT1**.
    Enter the maximum line width in the Line Width box.
  - Select **Graphics Printing** when using a laser printer; this prints one alarm per page.
    Click on the Font Name arrow and select the font: **Arial**, **Courier**, **Sans Serif** or **Times New Roman**.
    Click on the Font Style arrow and select a style: **Plain**, **Bold** or **Italics**.
    Enter the point size in the Font Size box—for example, **10** for 10-point type.
- In the Text to Print box, enter the message as you want it to appear, using the appropriate punctuation, including spaces and returns to separate lines of text.
- You can add dynamic alarm data to the text by selecting field codes from the Append Field Code list (see **Table 4** for definitions). To do this:
  - Place the cursor in the Text to Print box where you want the data to appear.
  - Click on the Append Field Code down arrow, then select an option from the drop-down list.
- When finished, click the **Accept** button (or **Cancel** to close the window without saving your changes).

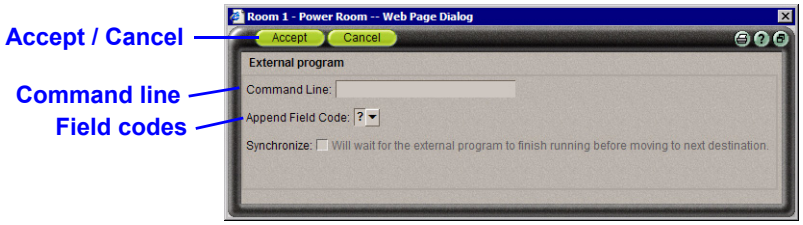
Once the action is set up, it appears in the **Actions** tab window. You may click the **Edit** button to make changes or the **Delete** button to remove it.

9.4.3 Run External Program Action

The Run External Program alarm action launches a script that starts a program or batch file on the server when an alarm is received.

Open the External Program window, shown below, to set up this action. To do this:

- Click the **GEO** button, then click on an item in the tree at left. When configured, the action will apply to the designated item in the tree as well as its subordinate items.
- Click the **Alarms** button, then the **Actions** tab.
- Select the alarm categories (**Step 1** in the **Actions** tab window) and alarm sources (**Step 2**) you want linked this action.
- Click on the down arrow (**Step 3**), select **Run External Program** from the drop-down menu and click **Add**.



- Enter the path of the executable file to be run followed by the path of the output file.

  For example:

  c:\windows\notepad.exe

  c:\SiteScan Web\output1.txt

  In the example, the program **Notepad** will be opened and a text file named **output1.txt** will be created in the **SiteScan Web** program folder on the server's **C: drive**
- Append Field Codes to the command line by choosing from the drop down list (see **Table 4** for definitions). More than one field code may be chosen (see example below).

  For example:

  c:\reports\run_report.bat $Generation_time$$To_State$

  This starts a batch file on the server and uses the alarm's **generation time** and **state** as values.
- Placing a check mark (✔) in the **Synchronize** box instructs SiteScan to wait until the external program has finished running before initiating the next **Run External Program** alarm action.
- When finished, click the **Accept** button (or **Cancel** to close the window without saving your changes).

Once the action is set up, it appears in the **Actions** tab window. You may click the **Edit** button to make changes or the **Delete** button to remove it.

9.4.4 Send Alphanumeric Page Action

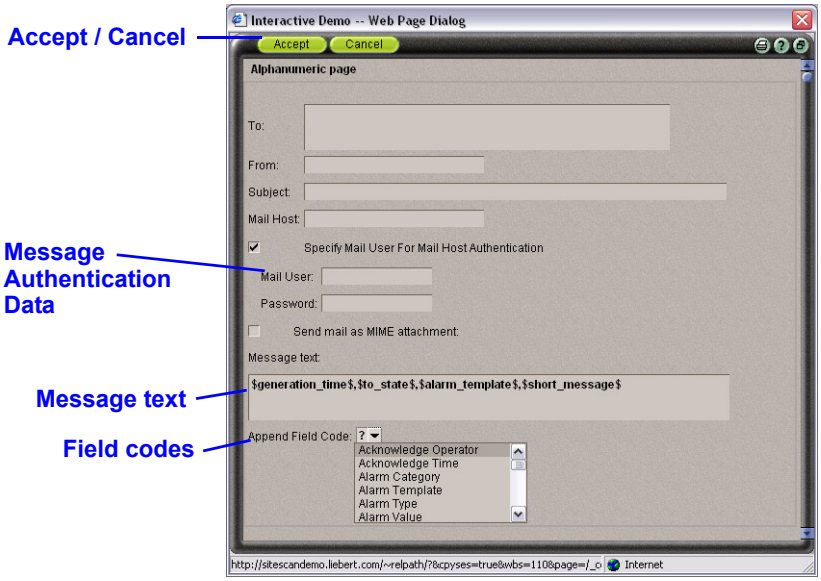
The Send Alphanumeric Page alarm action sends a page to one or more alphanumeric pagers or sends text messages to cell phones. The recipient's pager or phone must accept be able to accept e-mail.

Do not assign the Alphanumeric Page alarm action to frequently occurring alarms if you are using a stand-alone workstation. Sending pages for a frequently occurring alarm may dramatically slow down your system and cause problems with your mail server.

If the page will be sent over the Internet from a workstation that is not directly connected to the Internet, the workstation must first be configured to connect to the Internet automatically (see **Set Up a Dial-Up Networking Connection on page 23**).

Open the Alphanumeric Page window, shown below, to set up this action. To do this:

- Click the **GEO** button, then click on an item in the tree at left. When configured, the action will apply to the designated item in the tree as well as its subordinate items.
- Click the **Alarms** button, then the **Actions** tab.
- Select the alarm categories (**Step 1** in the **Actions** tab window) and alarm sources (**Step 2**) you want linked this action.
- Click on the down arrow (**Step 3**), select **Send Alphanumeric Page** from the drop-down menu and click **Add**.



- In the **To:** box, enter the service provider's phone number in this format: 1 800-555-1212. Do not use parentheses around the area code. More than one recipient may be specified.
- Enter a valid address, if required by your mailserver, in the **From:** box.
- Enter a subject of the notification in the **Subject:** box.
- Enter your Simple Main Transfer Protocol in the **Mail Host:** box. This can be either an IP address or a system name, such as mail.mycompany.com.
- If your mail server requires a user name and password, put a check mark (✔) in the **Specify Mail User** box. This opens the **Mail User** and **Password** boxes to accept the information.
- Put a check mark (✔) in the **Send mail as MIME attachment** box if your mail server allows only MIME attachments.
- Compose a message to be sent in the **Message Text** box, using punctuation, spaces and returns to format the text.
- Add live data to the message by selecting field codes from the **Append Field Code** list (see **Table 4** for definitions).
- When finished, click the **Accept** button (or **Cancel** to close the window without saving your changes).

Once the action is set up, it appears in the **Actions** tab window. You may click the **Edit** button to make changes or the **Delete** button to remove it.

Set Up a Dial-Up Networking Connection

A dial-up networking connection must be set up if the page will be sent over the Internet from a workstation that is not directly connected to the Internet. This enables SiteScan® Web to dial out to send an e-mail or alphanumeric page. After creating and executing an alarm action, the modem should dial automatically, then hang up after a minute of inactivity.

- Set up your server and modem to dial the default connection to your Internet Service Provider. See your server and modem documentation.
- Connect to the Internet and enter your Internet Service Provider's name and phone number, then your user name and password. Your modem must be detected before you can configure your Internet account connection.
- Type the following line at the end of the **system.properties** file in your system directory:
  repactions.connection.name=<name of connection>

9.4.5 Send E-Mail Action

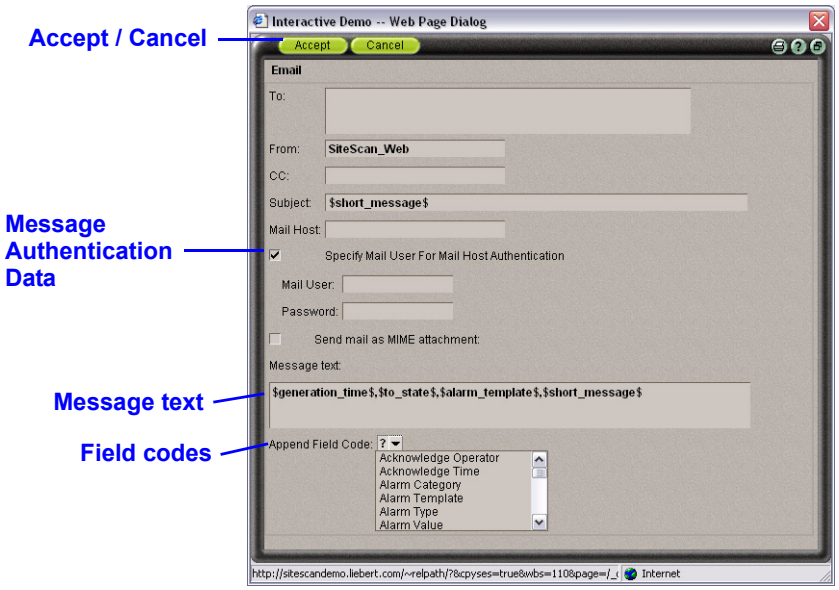
Use the Send E-Mail action to send customized e-mail messages to selected recipients when an alarm occurs.

Do not assign the Send E-Mail alarm action to frequently occurring alarms if you are using a stand-alone workstation. Sending pages for a frequently occurring alarm may dramatically slow down your system and cause problems with your mail server.

If the e-mail will be sent from a workstation that is not directly connected to the Internet, the workstation must first be configured to connect to the Internet automatically (see **Set Up a Dial-Up Networking Connection on page 23**).

Open the Email window, shown below, to set up this action. To do this:

- Click the **GEO** button, then click on an item in the tree at left. When configured, the action will apply to the designated item in the tree as well as its subordinate items.
- Click the **Alarms** button, then the **Actions** tab.
- Select the alarm categories (**Step 1** in the **Actions** tab window) and alarm sources (**Step 2**) you want linked this action.
- Click on the down arrow (**Step 3**), select **Send E-Mail** from the drop-down menu and click **Add**.



- In the **To:** box, enter the recipient's e-mail address. More than one recipient may be specified.
- Enter a valid address, if required by your mail server, in the **From:** box.
- Enter a subject for the e-mail notification in the **Subject:** box.
- Enter your Simple Main Transfer Protocol in the **Mail Host:** box. This can be either an IP address or a system name, such as mail.mycompany.com.
- If your mail server requires a user name and password, put a check mark (✔) in the **Specify Mail User** box. This opens the **Mail User** and **Password** boxes to accept the information.
- Put a check mark (✔) in the **Send mail as MIME attachment** box if your mail server allows only MIME attachments.
- Compose a message to be sent in the **Message Text** box, using punctuation, spaces and returns to format the text.
- Add live data to the message by selecting field codes from the **Append Field Code** list (see **Table 4** for definitions).
- When finished, click the **Accept** button (or **Cancel** to close the window without saving your changes).

9.4.6 Send an SNMP Trap Action

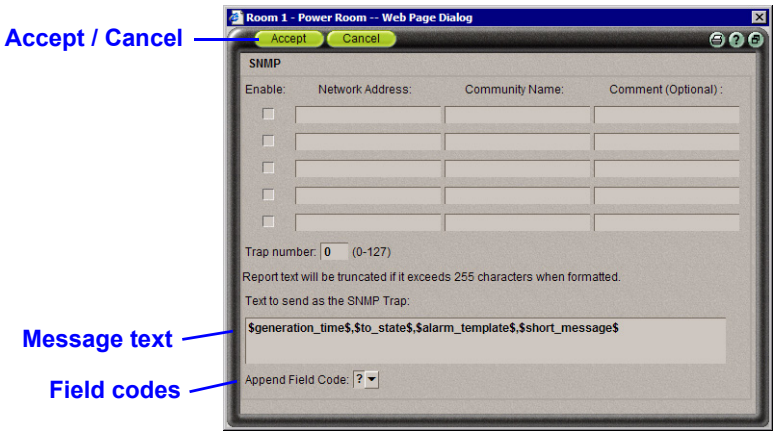
The Send SNMP Trap alarm action sends an SNMP trap in response to receiving an alarm. Traps contain the text created in the Text to send as the SNMP Trap field in the alarm action dialog box. You can configure up to five SNMP servers to receive traps.

SiteScan Web supports SNMP v1.

Each SNMP server chosen to receive these traps must have SNMP monitoring equipment installed. If problems arise with your SNMP connection or receiving traps, contact your information services department.

To set up this action, open the SNMP window, shown below. To do this:

- Click the **GEO** button, then click on an item in the tree at left. When configured, the action will apply to the designated item in the tree as well as its subordinate items.
- Click the **Alarms** button, then the **Actions** tab.
- Select the alarm categories (**Step 1** in the **Actions** tab window) and alarm sources (**Step 2**) you want linked this action.
- Click on the down arrow (**Step 3**), select **Send SNMP Trap** from the drop-down menu and click **Add**.



- Put a check mark (✔) in the **Enable** box and enter the SNMP server's network address community name in the appropriate boxes. Obtain this information from your network administrator.

  Deleting the check mark (✔) from an **Enable** box removes the attendant address from the SNMP trap notification.

  The **Comment (optional)** field may be used for the location of the SNMP server.
- **Trap number** box accepts a numeral from 1 to 127 to identify a message from this alarm action. This featured is used if trap numbers have been configured. Obtain this information from your network administrator. The same trap number is used for all messages from this alarm action.
- The **Text to send as the SNMP Trap** box will accept up to 255 characters. Longer messages will be truncated.

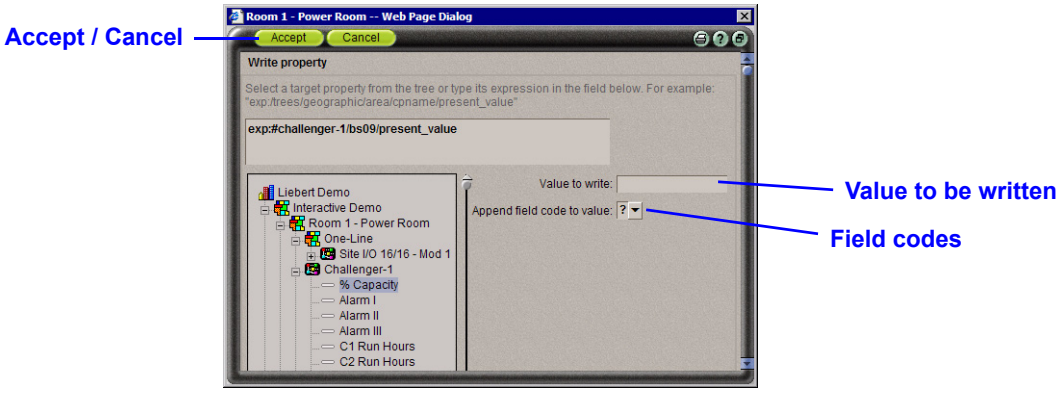
  Use punctuation, spaces and returns to format the message. You may customize the message by selecting field codes from the **Append Field Code** list (see **Table 4** for definitions).
- When finished, click the **Accept** button (or **Cancel** to close the window without saving your changes).

9.4.7 Write Property Action

The **Write Property** alarm action updates a microblock property value.

Open the Write Property window, shown below, to set up this action. To do this:

- Click the **GEO** button, then click on an item in the tree at left. When configured, the action will apply to the designated item in the tree as well as its subordinate items.
- Click the **Alarms** button, then the **Actions** tab.
- Select the alarm categories (**Step 1** in the **Actions** tab window) and alarm sources (**Step 2**) you want linked this action.
- Click on the down arrow (**Step 3**), select **Write Property** from the drop-down menu and click **Add**.



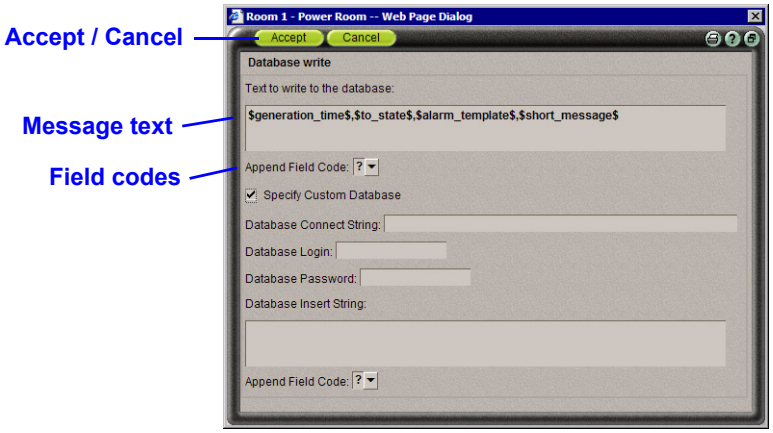
- In the **Value to Write** box, type the value you want to write to the microblock property. Type 0 or 1 for a binary property.
- Select field codes to add this information to the Value to Write field.
- When finished, click the **Accept** button (or **Cancel** to close the window without saving your changes).

9.4.8 Write to Database Action

The **Write to Database** alarm action stores alarm information in a table in the SiteScan Web alarm database or in a custom database. Third-party applications can access the alarm information for building maintenance management or alarm analysis. For example, an application can perform such actions as triggering a stored procedure or running a report.

Open the Database Write window, shown below, to set up this action. To do this:

- Click the **GEO** button, then click on an item in the tree at left. When configured, the action will apply to the designated item in the tree as well as its subordinate items.
- Click the **Alarms** button, then the **Actions** tab.
- Select the alarm categories (**Step 1** in the **Actions** tab window) and alarm sources (**Step 2**) you want linked this action.
- Click on the down arrow (**Step 3**), select **Write to Database** from the drop-down menu and click **Add**.



Writing to the SiteScan Web Alarm Database

When you add the **Write to Database** alarm action, by default SiteScan Web writes alarm information to the **write_db_ra** table in the SiteScan Web alarm database. The following table describes the information that SiteScan® Web writes to the database and gives the column name and data type you will need in order to access the alarm information from a third-party application.

Description	Column Name	Data type
Alarm generation time	EVENT_TIME_	Datestamp
Reference name path to the alarm source Example: #slm/m073	SOURCE_PATH_	String
Display name path to the alarm source Example: Atlanta Office/R&D Facility/Second Floor/VAV 2-1/Zone Temp	DISPLAY_NAME_	String
Alarm state Example: OFF NORMAL, LOW LIMIT, HIGH LIMIT	EVENT_STATE_	String
Alarm text as defined in the Text to write to the database field on the alarm action page. You can add live data to the text by selecting field codes from the **Append Field Code** list (see **Table 4** for definitions).	RA_TEXT_	String

To keep the database table from growing too large, you must delete old entries using a third-party database application. You cannot view, edit, or delete entries from SiteScan® Web.

NOTE

If your system uses an Access or MSDE database, you cannot open the database in a third-party application while SiteScan Web or SiteBuilder is running.

Writing to a Custom Database

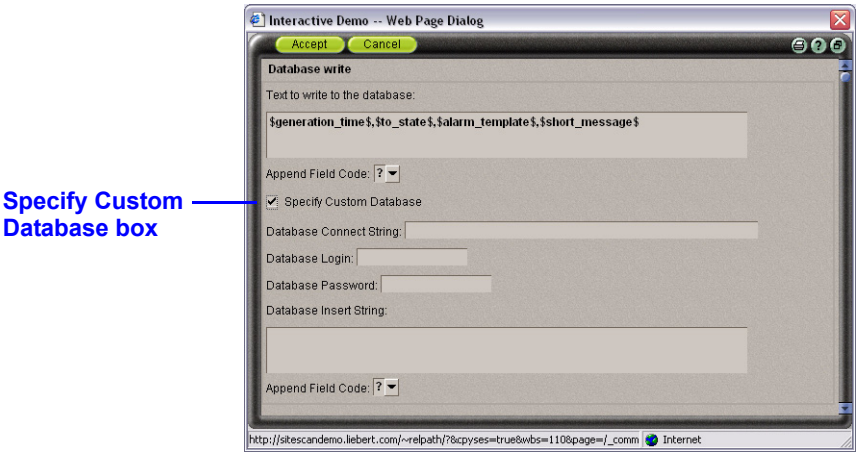
SiteScan Web can write alarm information to the following types of custom databases. The custom database does not have to be the same type as the SiteScan Web database.

- SQL Server
- MySQL
- PostgreSQL
- Oracle

You may create a table in an existing, third-party database or create a new database.

Using your database management tool, create a table in your custom database that includes fields for each alarm field code to be written to the table. Each field length in the table should be as long as the longest value to be written to that field.

To set up SiteScan Web to write to a custom database instead of to the SiteScan Web alarm database, select the **Specify Custom Database** check box on the Alarms page Actions tab, shown below, This reveals fields specifying how SiteScan Web writes to the database.



To enter the required information, refer to the following table.

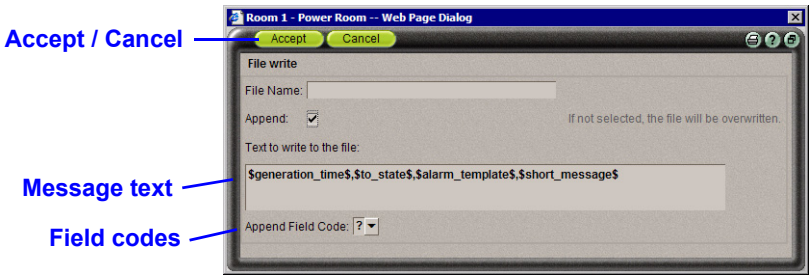
Field	Notes	
Text to write to the database	The text is made up of field codes that add live data to the text. You can select additional field codes from the Append Field Code list (see **Table 4** for definitions). NOTE: To write the text in this field to the custom database, you must include the Report Text field code ($report_text$) in the **Database Insert String** field described below.	
Database Connect String	**For database type:** SQL Server MySQL PostgreSQL Oracle	**The connect string format is...** jdbc:odbc:*<odbc_alias>* jdbc:mysql://*<host>:<port>/<instance>* jdbc:postgresql://*<host>:<port>/<instance>* jdbc:oracle:thin@*<host>:<port>/<instance>* where: *<host>* is the database server name/IP address *<port>* is the port number for the database *<instance>* is the database name in the database server *<odbc_alias>* is the name of the ODBC data source
Database Login and Password	The login and password to connect to the database.	
Database Insert String	Use the following format: Insert into <TABLE_NAME> (<column1_name>, <column2_name> ...) values (<$field_code1$>, <$field_code2$>, ...) Example: Insert into SiteScan® Web_ALARMS (TIME_, LOCATION_, TO_STATE_, TEXT_) values ($generation_time$, $location_path$, to_state, $report_text$) NOTE: You can add field codes to the Insert String using the Append Field Code list. If you add a timestamp type field code (for example, $generation_time$), you should have the data go into a timestamp data type field in the custom database. Otherwise, you must use field code formatting to format the time.	

9.4.9 Write to File Action

The Write to File action allows you to record alarm information in a file.

Open the File Write window, shown below, to set up this action. To do this:

- Click the **GEO** button, then click on an item in the tree at left. When configured, the action will apply to the designated item in the tree as well as its subordinate items.
- Click the **Alarms** button, then the **Actions** tab.
- Select the alarm categories (**Step 1** in the **Actions** tab window) and alarm sources (**Step 2**) you want linked this action.
- Click on the down arrow (**Step 3**), select **Write to File** from the drop-down menu and click **Add**.



- Enter a name in the File Name box.
- Click to place a check mark (✔) in the Append box to add new entries at the end of the file

  Note: If you do not check the Append box, the file contents will be overwritten with each new alarm message.
- In the Text to Write to the File box, enter the message as you want it to appear, using the appropriate punctuation, including spaces and returns to separate lines of text.
- You can add dynamic alarm data to the text by selecting field codes from the Append Field Code list (see **Table 4** for definitions). To do this:
  - Place the cursor in the Text to Write to the File box where you want the data to appear.
  - Click on the Append Field Code down arrow, then select an option from the drop-down list.
- When finished, click the **Accept** button (or **Cancel** to close the window without saving your changes).

Once the action is set up, it appears in the **Actions** tab window. You may click the **Edit** button to make changes or the **Delete** button to remove it.

9.4.10 Field Code Definitions

Table 4 shows the field codes displayed in Action and Messages windows.

Table 4 Field code definitions

Field Code Name	Field Code	Definition
Acknowledge Operator	$acknowledge_operator$	The operator who acknowledged the alarm.
Acknowledge Time	$acknowledge_time$	The time when the operator acknowledged the alarm.
Alarm Category	$event_category$	The alarm category that the alarm is assigned to.
Alarm Template	$event_template$	The alarm template that the alarm is assigned to.
Alarm Type	$event_type$	The alarm type of the alarm source; for example, CHANGE OF VALUE, CHANGE OF STATE.
Alarm Value	$alarm_value$	The alarm value.
Alert Text	$alerttext$	For a converted SuperVision system if the option **Create a single alarm template...** was selected during upgrade. Retrieves alarm message text from **cmnet_alert_text.properties**.
		To use this field code:
		1. Select the **Alert Text** field code.
		2. After $alerttext, type one of the following:
		:normalshort
		:normallong
		:alarmshort
		:alarmlong
		For example, $alerttext:alarmlong$
Character	c	A single ASCII character. Often used for form feeds and other printer escape sequences. For example, $C:65$ displays A.
Command Value	$command_value$	The commanded value from the alarm source. Valid only for alarm type COMMAND FAILURE.
Dead Band	$deadband$	The deadband value from the alarm source. Valid only for alarm type OUT-OF-RANGE.
Deletion Operator	$deletion_operator$	The operator who deleted the alarm.
Deletion Time	$deletion_time$	The time the alarm was deleted.
Device	$device$	The display name of the device where the alarm came from.
Equipment	$equipment$	The display name of the equipment where the alarm came from.
Error Limit	$error_limit$	The error limit, from the alarm source. Valid only for alarm type FLOATING LIMIT.
Exceeded Limit	$exceed_limit$	The exceeded limit value from the alarm source. Valid only for alarm type OUT-OF-RANGE.
Exceeding Value	$exceeding_value$	The exceeding value from the alarm source. Valid only for alarm type OUT-OF-RANGE.
Fault	$fault$	The status of the fault condition from the alarm source.
Feedback Value	$feedback_value$	The feedback value from the alarm source. Valid only for alarm type COMMAND FAILURE.
Field Message	$field_message$	Additional text recorded in the alarm by the device.
From State	$from_state$	The previous state of the alarm source.
Generation Operator	$generation_operator$	The operator who forced the alarm to return to normal.
Generation Time	$generation_time$	The time in the module when the alarm was generated.
In Alarm	in_alarm	The in alarm status from the alarm source.
Incident Closed Time	$incident_closed_time$	The time the alarm's entire incident group closed.

Table 4 Field code definitions

Field Code Name	Field Code	Definition
Latched Data Value (Analog)	$latched_data_analog:x$	“x” ranges from 1 to 5. The display name of the alarm source that generated the alarm.
Latched Data Value (Digital)	$latched_data_digital:x$	“x” ranges from 1 to 5. The display name of the alarm source that generated the alarm.
Location Path	$location_path$	Displays all the path display names from root to source.
Long Message	$long_message$	The formatted alarm long text displayed by double-clicking the alarm on the Alarms page.
Message Details	$message_details$	The message details displayed on the Alarms page **View** tab.
Message Prefix	$message_prefix$	The message prefix displayed on the Alarms page **View** tab.
Message Text	$message_text$	The message text displayed on the Alarms page **View** tab.
New State	new_state	The status of new state from the alarm source.
New Value	new_value	The new value from the alarm source. Valid only for alarm type CHANGE OF VALUE.
Object ID	$object_ID$	Object ID of the alarm source.
Out of Service	$out_of_service$	The status of 'out of service' from the alarm source.
Overridden	$overridden$	The status of 'overridden' from the alarm source.
Program ID	$program_id$	The address of the control program that generated the alarm. BACnet program address format: device ID, program number (example: 240219,5) SuperVision program address format: site, gateway, module, fb (example: 1, 2, 13, 5)
Receive Time	$receive_time$	The time at the workstation when the alarm was received.
Recipient Device ID	$device_id$	The device ID of the device where the alarm came from.
Record Type	$record_type$	The type of alarm; for example, BACnet, SuperVision, System.
Reference Path	$reference_path$	Path to alarm source. Available in all alarm actions.
Reference Value	$reference_value$	The 'reference value' from the alarm source. Valid only for alarm type FLOATING LIMIT.
Referenced Bitstring	$referenced_bitstring$	The value of the 'referenced bitstring' value from the alarm source. Valid only for alarm type CHANGE OF BITSTRING.
Report Text	$report_text$	Used only with the **Write to Database** alarm action. You must include this field code in the **Database Insert String**.
RTN Time	RTN_time	The time when the alarm returned to normal.
Setpoint Value	$setpoint_value$	The 'setpoint value' from the alarm source. Valid only for alarm type FLOATING LIMIT.
Short Message	$short_message$	The formatted alarm short text.
Site	$site$	The display name of the site the alarm came from.
Source	$source$	The display name of the alarm source that generated the alarm.
Source description	$source:description$	The description of the alarm source that generated the alarm.
Source Path	$source:<path>$	For advanced users, displays the database item indicated by <path> relative to the alarm source; for example, <path> = ~equipment.display-name. The easiest way to display the path is to use Global Modify.
System Directory	$system_dir$	The system folder name.
To State	to_state	The current state of the alarm source; for example, Normal, Fault, Off-normal, High limit, Low limit.

9.5 Enable/Disable

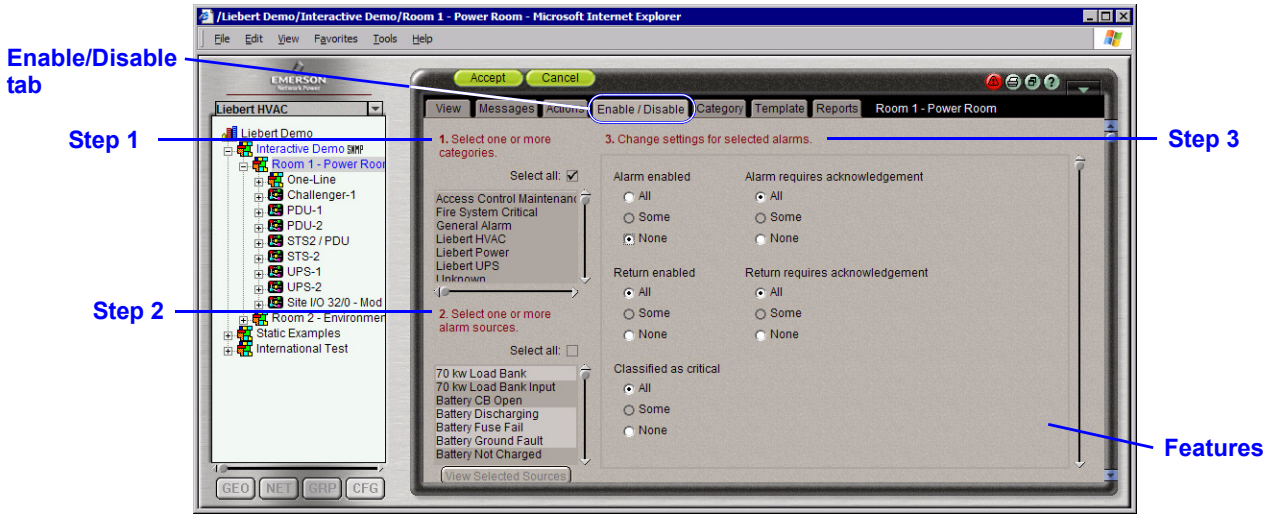
The **Enable/Disable** tab in the Alarms window allows you to customize the treatment of alarms and return-to-normal events for selected alarm sources. Through this function, you may:

- Activate or deactivate alarms and return-to-normal events
- Classify alarms as critical or non-critical
- Specify whether an operator must acknowledge alarms and return-to-normal events

9.5.1 Enable or Disable Features

To access the Enable/Disable functions:

- Click the **GEO** button, then click on an item in the tree at left.
- Click the **Alarms** button, then the **Enable/Disable** tab. Steps are listed in red, as shown below.



1. Select the categories that contain the alarm sources you want to set up.
2. Select the alarm sources for the selected categories.
   Note: In **Steps 1** and **2**, control-click to select multiple items, or click the Select All check box.
3. To change settings for the selected alarm sources, click on the **All** or **None** radio button for each of the following features:

Feature	If you click **All** to enable this feature, SiteScan Web:
• **Alarm enabled**	Generates an alarm when specified conditions occur in the alarm source.
• **Return enabled**	Generates a return-to-normal when the alarm source returns to a normal state.
• **Classified as critical** *	Changes the system-wide alarm button to red when an alarm occurs. Critical alarms that pass through a modem are delivered to the SiteScan Web server immediately.
• **Alarm requires acknowledgement**	Requires that an operator acknowledge the alarm.
• **Return requires acknowledgement**	Requires that an operator acknowledge the return-to-normal event.

* Note: If the **Classified as critical** feature is disabled (**None** button selected), SiteScan Web changes the system-wide alarm button to yellow when an alarm occurs. Non-critical alarms that pass through a modem are stored in the gateway until one of the following happens:

- A critical alarm occurs.
- The gateway is contacted by SiteScan Web.
- The gateway buffer is full, at which time all alarms are sent to SiteScan Web.

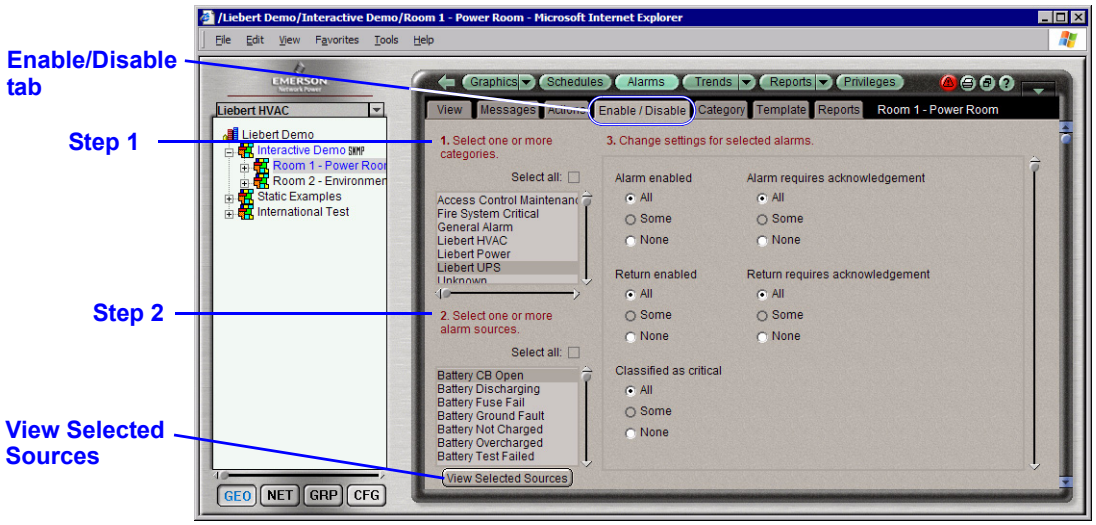
- When finished, click the **Accept** button (or **Cancel** to close the window without saving your changes).

9.5.2 View Selected Sources

In the **Enable/Disable** tab, you may use the **View Selected Sources** button to view a listing of all selected alarm sources in a dialog box where you may enable or disable features for any source.

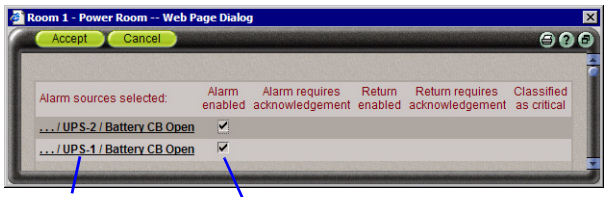
To access the Enable/Disable functions:

- Click the **GEO** button, then click on an item in the tree at left.
- Click the **Alarms** button, then the **Enable/Disable** tab. Steps are listed in red, as shown below.

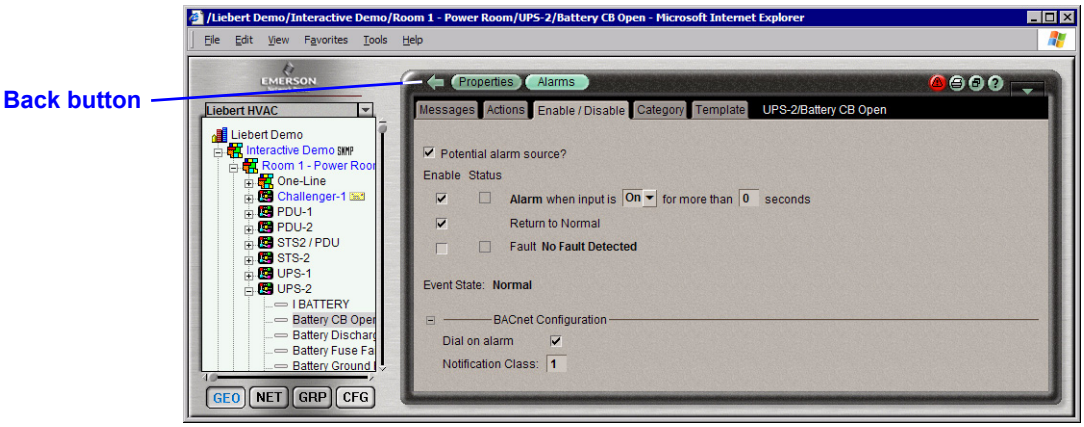


- In the **Enable/Disable** tab window:
  1. Select the categories that contain the alarm sources you want to view.
  2. Select the alarm sources for the selected categories.

     Note: In **Steps 1** and **2**, control-click to select multiple items, or click the Select All check box.
  3. Click the **View Selected Sources** button.
- A dialog box appears, listing all selected alarm sources with check boxes for enabled features, as shown at right. Use the scroll bar as needed to view additional sources.
- To enable a feature, click to place a check mark (✔) in the box. To disable a feature, click to remove the check mark.
- When finished, click **Accept** (or **Cancel** to close the window without saving your changes).


Room 1 - Power Room -- Web Page Dialog
Accept
Cancel
Alarm sources selected:
Alarm enabled
Alarm requires acknowledgement
Return enabled
Return requires acknowledgement
Classified as critical
. . . / UPS-2 / Battery CB Open
. . . / UPS-1 / Battery CB Open
Link to details
Enable or disable feature

- You may click on an alarm source to view more complete information, as in the example below. Note the tree at left shows the alarm source selected in the tree. Click the Back button to return to the previous view.

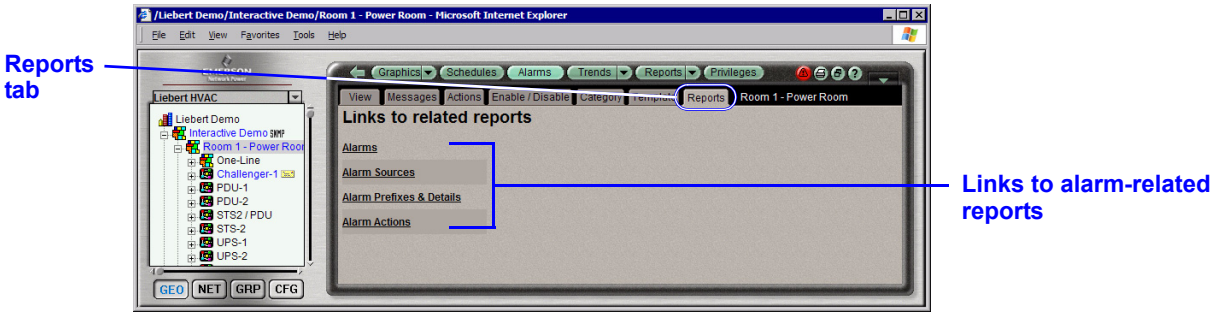


9.6 Alarm Reports

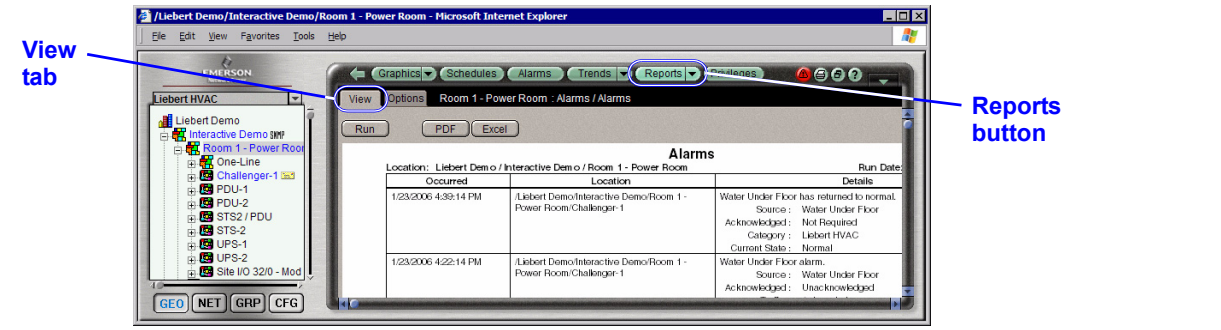
The **Reports** tab in the Alarms window offers quick access to four alarm-related reports. These four reports are also accessible from the **Reports** menu action button.

To access Reports from the Alarms window:

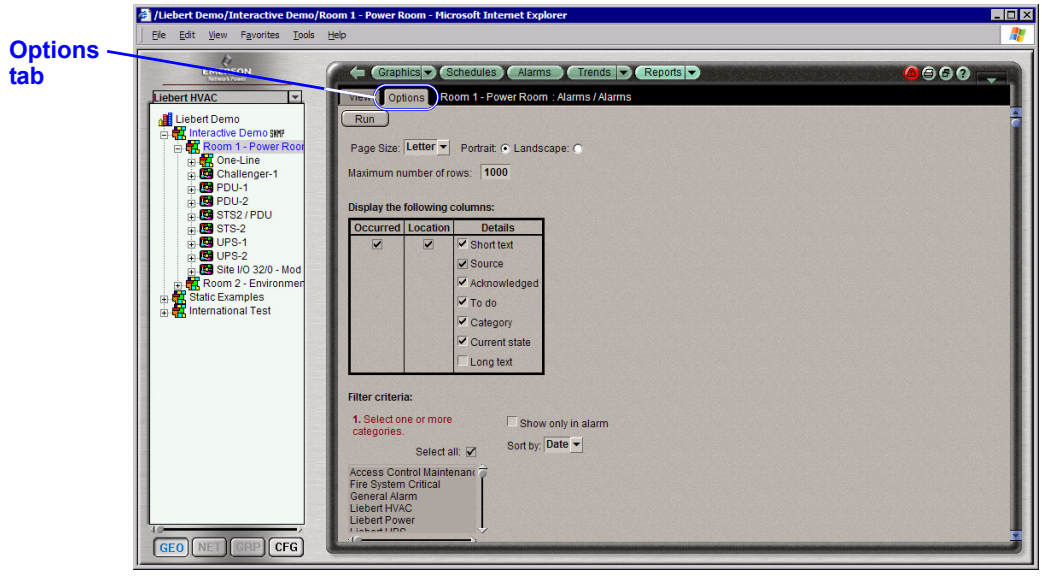
- Click the **GEO** button, then click on an item in the tree at left.
- Click the **Alarms** button, then the **Reports** tab.



- Click on a link to a report you want to view. The Reports window opens, as shown below, with the **Reports** button is highlighted. Click the **View** tab to see the report.



- Click the **Run** button to generate a new report. When the report is displayed, you may copy the report contents to a file:
  - Click the **PDF** button to create a PDF file that may be opened with Adobe® Acrobat®.
  - Click the **Excel** button to generate a Microsoft® Excel spreadsheet.
- Click the **Options** tab to view or change the report settings. See **11.2 - Set Up Report Options** for details about this window.



10.0 VIEWING TRENDS

SiteScan Web can read and store equipment status values over time and then display this information in a graph to help you monitor the equipment's operation.

Trend data can be collected for any BACnet input or output point in SiteScan Web. The control module reads values for a point at intervals that you define and then stores that data in the module.

Because a control module has limited memory for storing trend data, you can set up historical trending to archive the trend data from the module to the SiteScan Web database. A trend graph can display data from both the control module and the database.

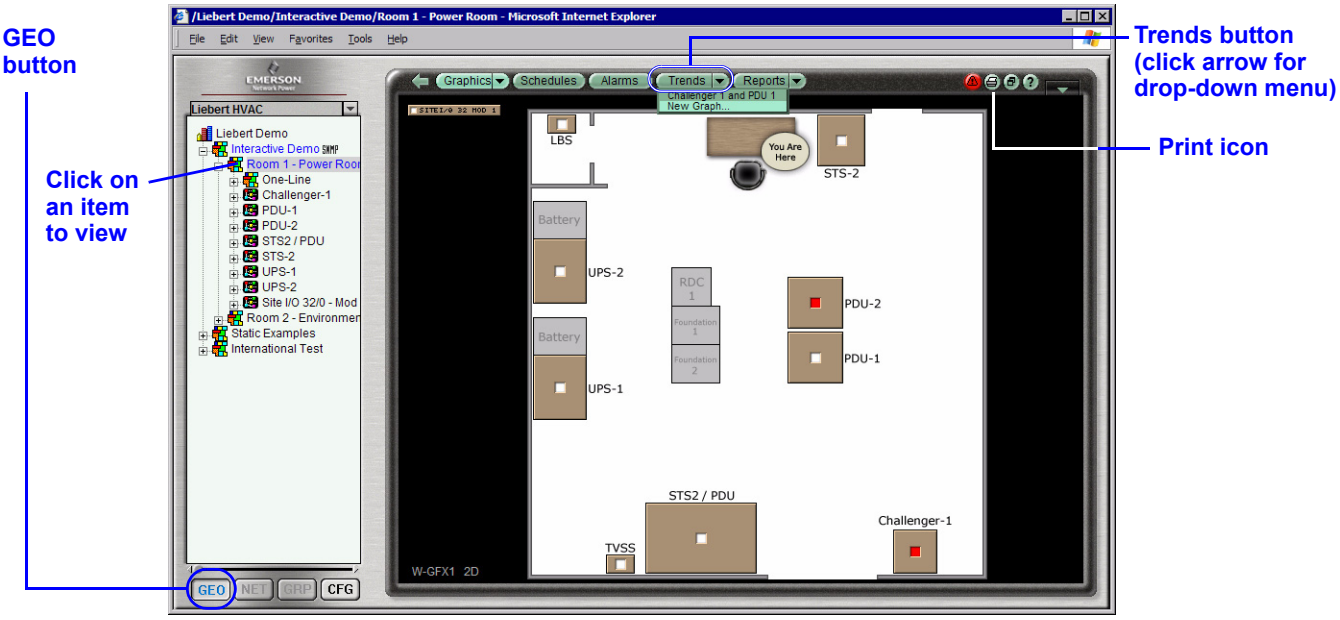
Note: You can also access trend data in the database using ODBC/SQL queries.

10.1 View Trends

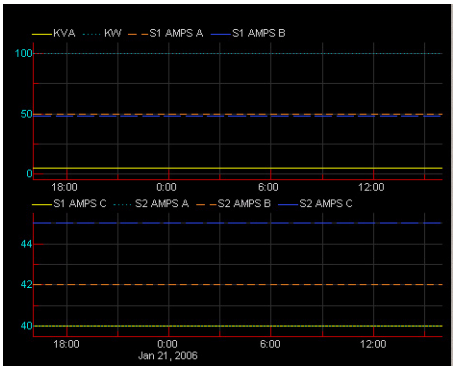
In SiteScan Web, you can view and print trend graphs. You can also copy the trend data to a spreadsheet program.

To view a trend graph:

- Click the **GEO** button in the bottom left corner.
- In the tree at left, click on the equipment that has the trends you want to view.
- Click the **Trends** menu action button down arrow, then select the point graph or custom graph you want to print from the drop-down menu.



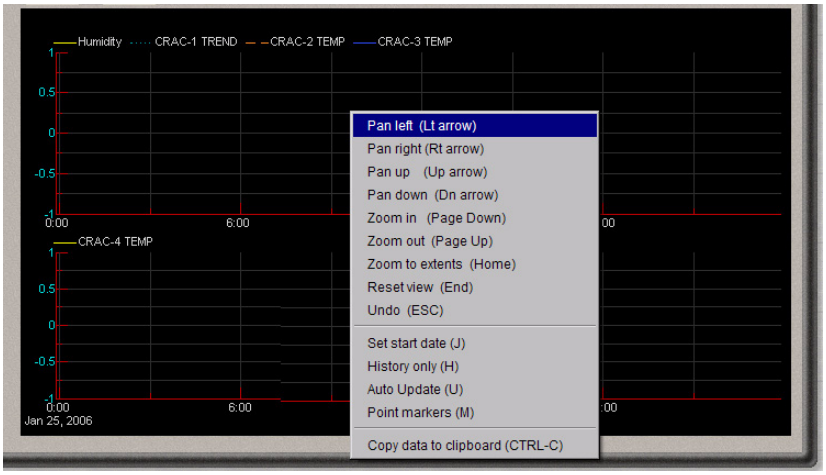
- Click the **View** tab to display the graph.
  There will be a delay as SiteScan Web collects data for the graph. The graph appears, as shown in the example at right.
- For tips on viewing the graph, see **10.1.1 - Tools for viewing trends**.
- Click the **Print** icon in the top right corner of the Trends window to print the graph.



10.1.1 Tools for viewing trends

Some tips for viewing trend graphs follow:

- A vertical dashed line indicates missing data.
- A large marker indicates a point that is in alarm, in fault, out of service or has been overridden. Control-click the marker to view details.
- Right-click anywhere on a trend graph to display a popup menu with tools described in **Table 5**. Click on an item in the popup menu or use the keyboard shortcut shown in parentheses () on the menu.



- **Table 5** shows commands available from the popup menu shown above and two other options.

Table 5 Tools for viewing trend graphs

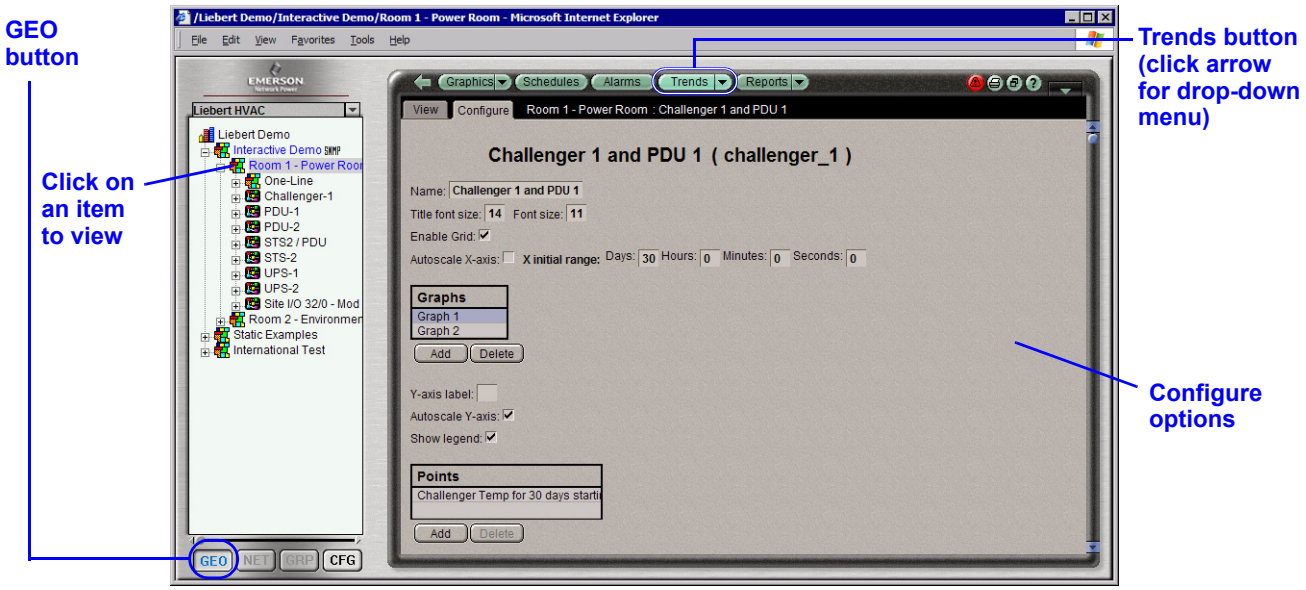
Tool	Keyboard Shortcut	Notes
Pan	Arrow keys	If you display more than one graph, panning up and down affects only one graph at a time. Panning left to right affects all graphs. You can also Alt+click and drag inside the graph.
Zoom in	Page Down	You can also use the plus (+) key on the numeric keypad, the **X** key, or drag a rectangle around area.
Zoom out	Page Up	You can also use the minus (-) key on the numeric keypad or the **Z** key.
Zoom to extents	Home	Shows all the data you have viewed in the current session of a particular trend graph.
Reset view	End	Resets the display to its default setting. You can also use the Enter or **R** key.
Undo	Esc	Undo up to 10 changes to your view.
Set start date	J	Enter the date you want the trend to jump to. The trend displays the same time range for the new date. Press the **J** key again to hide the date fields.
History Only	H	Displays only the historical data on the graph.
Auto Update	U	The trend graph polls for data every 10 seconds. Press **U** again to stop updating.
Point Markers	M	Shows a marker for each data point in the graph.
Copy	Ctrl+C	Copies only the data from the time range that is currently displayed.
Other Options ***(not available on the popup menu)***		
Refresh the display (gather trend data)	—	Click the **Trends** button.
Display data for a specific sample	—	Ctrl+click a sample to view the point name, time and date the sample was read, the exact point value, and if the point is in alarm, is in fault, out of service, or has been overridden. Click anywhere to clear the details.

10.2 Configure Trends

The **Configure** tab in the Trends window allows you to specify options for the trend graph.

To configure a trend graph:

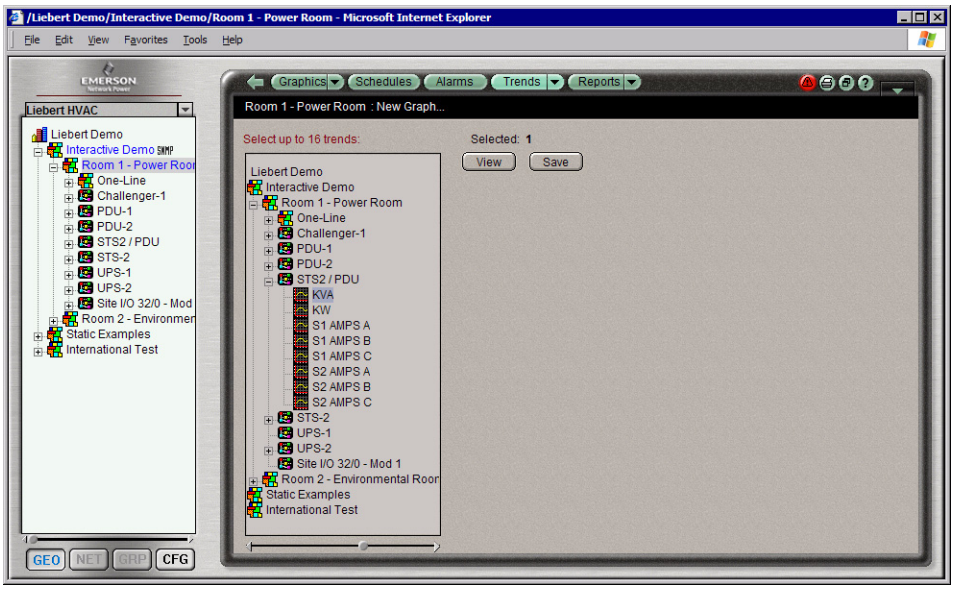
- Click the **GEO** button in the bottom left corner.
- In the tree at left, click on the equipment that has the trends you want to set up.
- Click the **Trends** menu action button down arrow, then select the point graph or custom graph you want to print from the drop-down menu.
- Click the **Configure** tab.



Set up the desired options for trend graph.

10.3 Create a New Trend Graph

- Click the **GEO** button in the bottom left corner.
- Click on an item in the tree at left.
- Click the **Trends** button down arrow, then select **New Graph** from the drop-down menu.



- Click to select up to 16 items for the trend graph.
- Click **View** to see the graph or **Save** to save the new graph and place it on the Trends menu.

11.0 VIEWING REPORTS

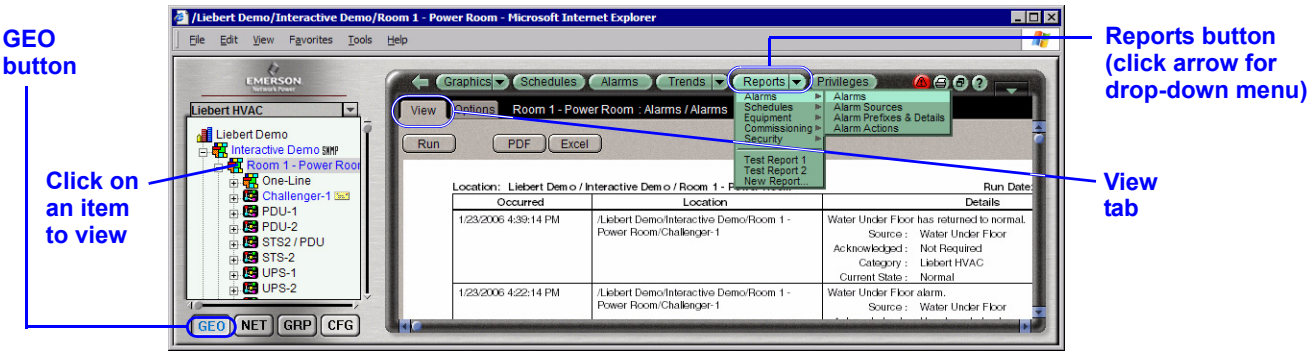
The **Reports** button offers a quick way to compile alarm and other information to help manage and troubleshoot your system. You may access existing reports (see **Table 6**) or generate a new report.

Table 6 Available reports

Alarms	Schedules	Equipment	Commissioning	Security
• Alarms • Alarm Sources • Alarm Prefixes & Details • Alarm Actions	• Schedule Instances • Effective Schedules	• Point List • Locked Values • Network IO • Trend Usage • Parameter Mismatch	• Test & Balance • Equipment Checkout	• Audit Log • Security Assignments

11.1 View Reports

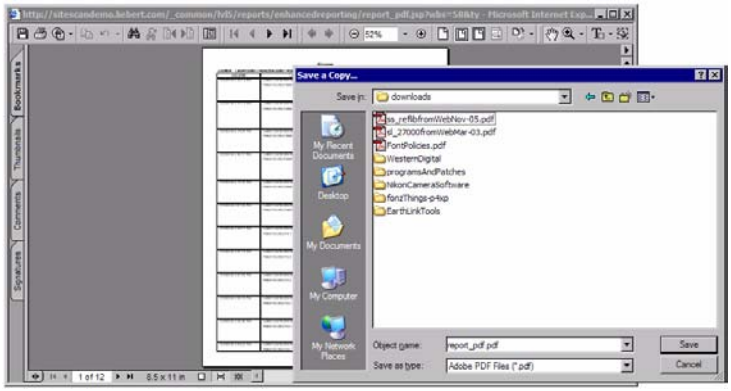
- Click the **GEO** button in the bottom left corner.
- Click on an item in the tree at left—**Room 1 Power Room** in the example below.
- Click the **Reports** menu action button at the top. The Reports window has two tabs across the top; the example below shows the **View** tab.



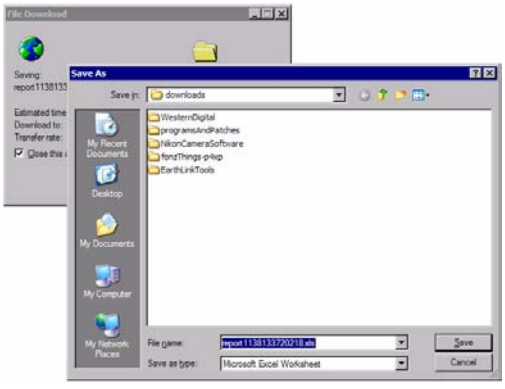
- To view an existing report, click on the Reports down arrow, then click on a category to display a submenu and select a report.
- Click the **Run** button below the **View** tab to generate a report. There might be a delay, depending on the report request; during this time, the message *Report Running* is displayed.
- When the report is displayed, you may copy the report contents to a PDF or Excel file.

  To create a PDF:
  - Click the **PDF** button to create a PDF file that may be opened with Adobe Acrobat. An Acrobat program window opens with the PDF in view.
  - Click the **Save** button to open the Save a Copy window, shown below left.
  - Specify where to save the file and a file name. Click the **Save** button to save the file.

  To create an Excel file:
  - Click the **Excel** button to generate a Microsoft Excel spreadsheet. A File Download message may ask whether to continue, depending on your settings. Click **Save** to continue.
  - In the Save As window, shown below right, choose where to save the file and specify a file name. Click the **Save** button to download the file.



SAVE REPORT AS A PDF



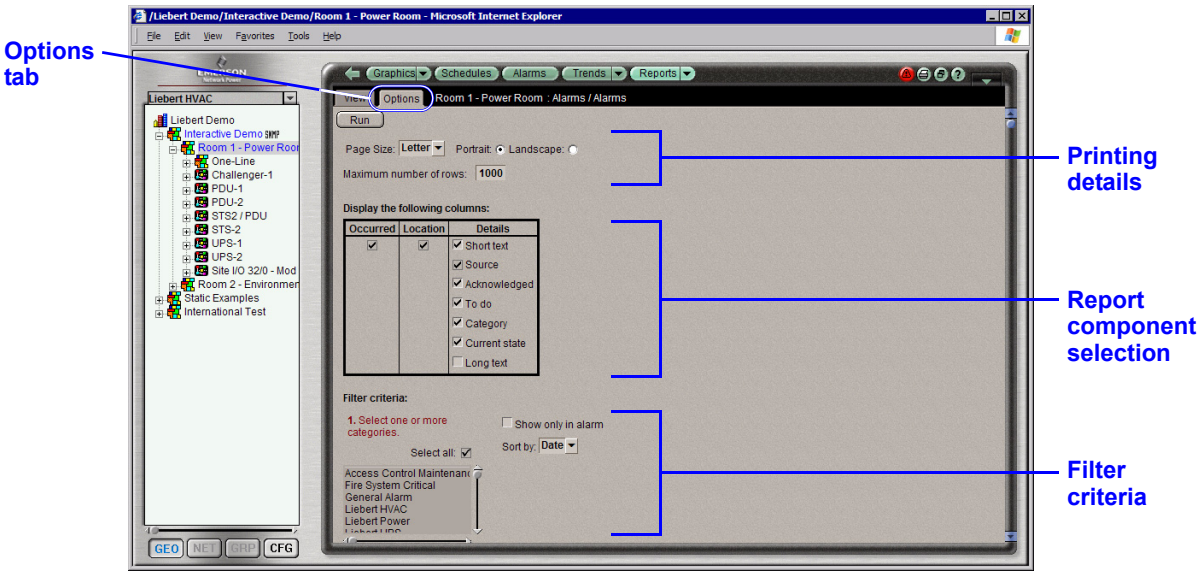
SAVE REPORT AS AN EXCEL FILE

11.2 Set Up Report Options

The Reports **Options** tab allows you to customize reports. For all report types, you may specify page size, orientation and maximum length. Other options vary by type of report.

To access the report Options functions:

- Click the **GEO** button, then click on an item in the tree at left.
- Click the **Reports** button, then the **Report Options** tab.



- The Options tab window has three main sections:
  - Printing details
  - Report component selection (not available for all report types)
  - Filter criteria (choices vary by report type)
- In the **Printing details** section:
  - Specify the size of the report page by clicking the Page Size down arrow and selecting an option from the drop-down list—for example, **Letter**, **Legal** or **A4**.
  - Choose the orientation by clicking on **Portrait** or **Landscape**.
  - Specify the maximum number of rows to appear in the report—in the example above, **1000**. This may be helpful to reduce the size of reports you expect to be excessively long.
- In the **Report component selection** section:
  - For some report types, you may choose which report components to show or hide in the **Display the following columns** table.
  - Click to place a check mark (✔) for items you want to include; click to remove the check mark for items you want to omit. Some check boxes may be grayed-out; these items may not be changed.
- In the **Filter criteria** section:
  - Many report types allow you to choose criteria to filter the report. In the example above, you may select the categories that contain the alarm sources you want to view. Control-click to select multiple items, or click to place a check mark (✔) in the Select All check box.
  - For alarm reports, you may choose to include only those items that are currently in alarm. To do this, click to place a check mark (✔) in the **Show only in alarm** check box. (Leave the check box blank to include all items.)
  - If there is an option to sort the report, click on the Sort By arrow and select an option from the drop-down menu—in the example above, **Date** or **To Do**.
- When finished, click **Accept** (or **Cancel** to close the window without saving your changes).
- At any time, click on the **Run** button to view the report.

11.3 Set Up a New Report

In addition to the standard reports available from the **Reports** button drop-down menu, SiteScan Web provides three basic templates for you to design a new report:

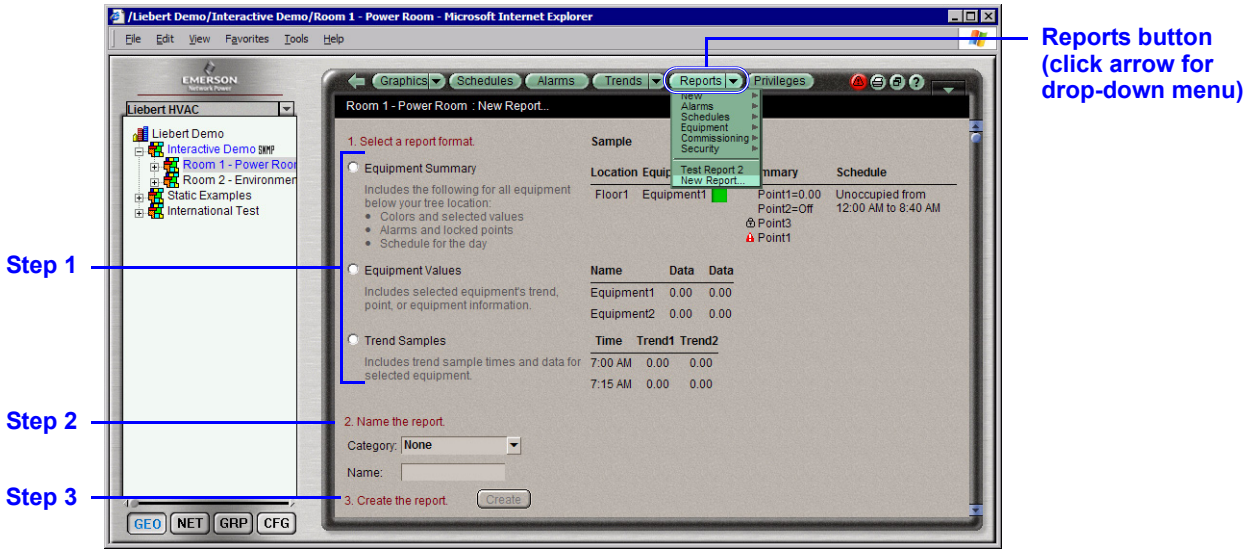
- Equipment Summary
- Equipment Values
- Trend Samples

Once a new report is set up, it appears on the **Reports** drop-down menu. See **11.1 - View Reports** for details on all the functions available after the new report appears on the menu.

After creating a new report, the **Options** tab changes to the **Design** tab. At any time, you may select the report and click on the **Design** tab to make additional changes.

To set up a new report:

- Click the **GEO** button, then click on an item in the tree at left.
- Click the **Reports** button arrow, then click on **New Report** in the drop-down menu. Steps are listed in red, as shown below.



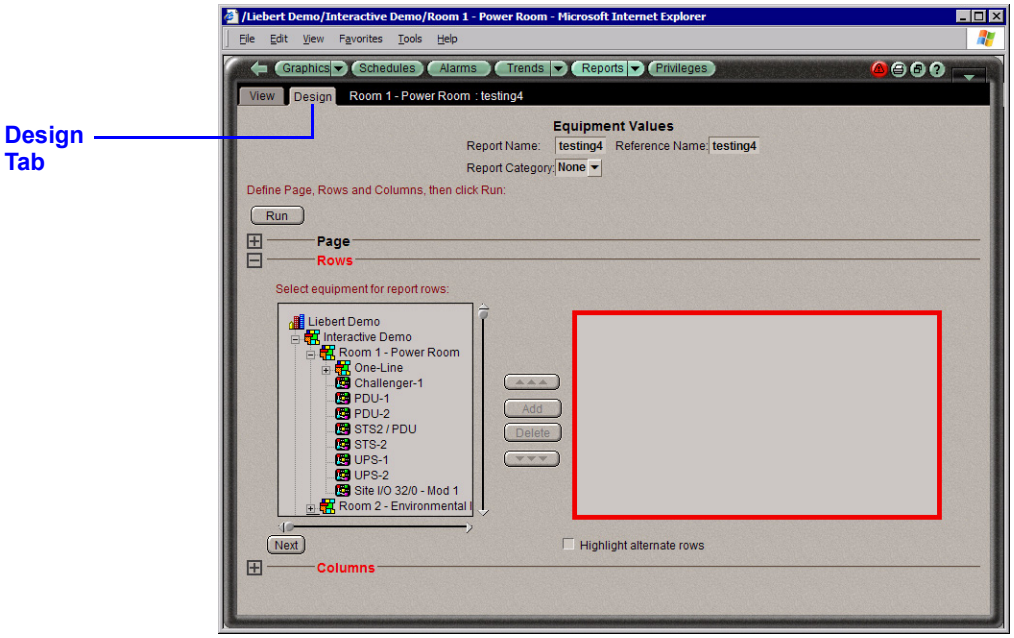
11.3.1 Create a New Report

1. Choose a report format by clicking on one of the radio buttons: **Equipment Summary**, **Equipment Values** or **Trend Samples**. Each format is described and shown in the window.
2. In the Name box, enter a report name as you want it to appear on the **Reports** drop-down menu.

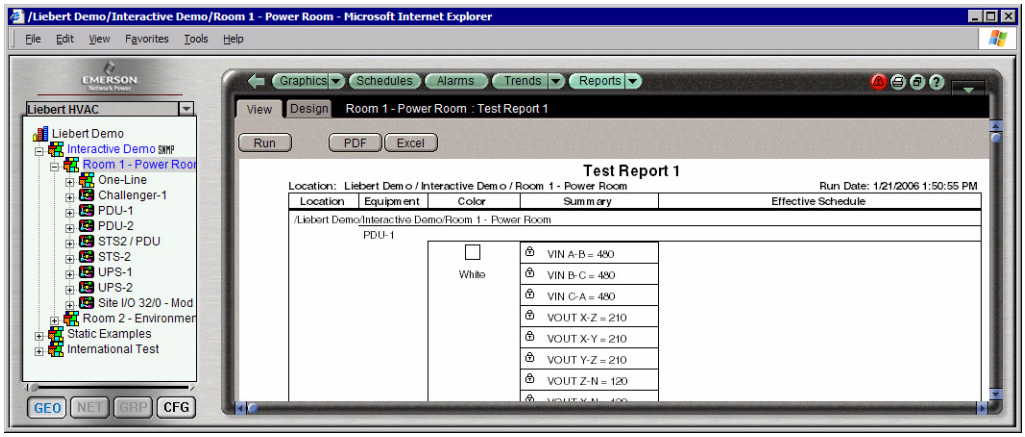
   Note: If you have created report categories via the CFG Categories function, you may click on the **Category** arrow and select an option from the drop-down menu.
3. Click the **Create** button to create the new report. The **Options** tab label changes to **Design**. To design the new report, proceed to the next section, **11.3.2 - Design the New Report**

11.3.2 Design the New Report

After you create a new report, the Design tab replaces the Options tab, as shown below.



- The top center portion of the window displays the report type, name and other identifying information.
- Each report type has three sets of options that you may change: Page, Rows and Columns. Items shown in red text require choices. In the example above, setup is required for Rows and Columns. The changes must be made in order from top to bottom. For example, you must set up the Rows options before you can define the Columns settings.
- Click on the plus (+) sign to expand the Page, Rows or Columns options. Click the minus (-) sign to hide the options.
- When all required items in a category are completed, the red text for that category changes to black. You may continue to make changes after the red text changes to black.
- When finished, click **Accept** (or **Cancel** to close the window without saving your changes).
- At any time, click on the **Run** button to view the report. An example is shown below.



11.4 Description of SiteScan Web Reports

The reports available in SiteScan Web are described in **Table 7**.

Table 7 Description of available reports

Report	Description
Alarms	
Alarms	View, sort and filter the information displayed in the Alarms **View** tab.
Alarm Sources	Create a summary of potential alarm sources configured in the Alarms **Enable/Disable** tab.
Alarm Prefixes & Details	Create a summary of the information configured in the Alarms **Messages** tab.
Alarm Actions	Create a summary of the information configured in the Alarms **Actions** tab.
Schedules	
Schedule Instances	Find every schedule entered at and below a selected tree item. This report shows the location of each item and can help you find newly added and conflicting schedules.
Effective Schedules	View all equipment that may be scheduled and the net result of all schedules in effect for a selected date and time.
Equipment	
Point List	View the details of all points and verify that all points were checked out during commissioning. Create custom lists for other contractors, such as a list of BACnet IDs or Web services links.
Locked Values	Find all locked points and locked values.
Network IO	Verify the programming and status of all network points—especially useful for commissioning control modules used for third-party integration.
Trend Usage	Create a summary of the information configured in the Trends **Enable/Disable** tab.
Parameter Mismatch	Find out whether your system has any parameter mismatches that need to be resolved.
Commissioning	
Test & Balance	View the results of VAV box commissioning.
Equipment Checkout	View the information on the **Equipment Checkout** tab of the Point Checkout tool during commissioning. Also, find equipment that has not been fully commissioned.
Security	
Audit Log	Create a chronological list of operators with property changes they have made and the reasons for those changes.
Security Assignments	View a list of locations showing which operators are assigned to each location and their privilege sets.

12.0 CONFIGURING SITESCAN WEB

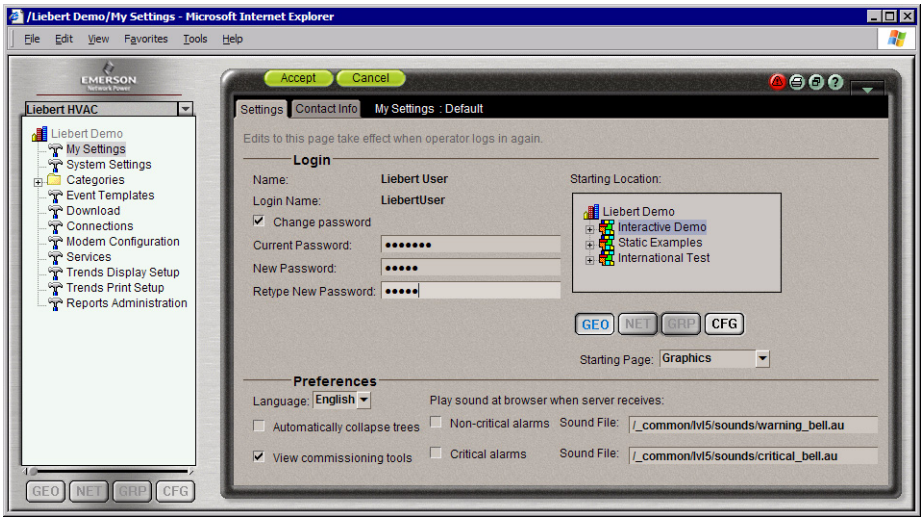
Most of the configuration for SiteScan Web is performed by LGS. This section provides instructions on how to change the most commonly used configuration settings.

12.1 My Settings

My Settings has two tabs: **Settings** and **Contact Info**.

12.1.1 Settings

- Click on the **CFG** button, then click on **My Settings** in the tree at left.
- Click on the **Settings** tab to display the following window.



Change Password

To change the login password:

- In the Login section, click to place a check mark (✔) in the Change Password box.
- Enter the existing password in the Current Password box.
- Enter the new password in the New Password box. The password is case-sensitive.
- Confirm the new password by re-entering it in the Retype New Password box.
- Click the **Accept** button to save your changes.

Change Starting Location

To specify the view that SiteScan Web displays after you log in:

- Click on an item in the tree below Starting Location. Click the plus (+) sign to expand an item.
- Click on the view button—for example, **GEO** or **CFG**—to be active when SiteScan Web starts.
- Click on the Starting Page arrow and select an option from the drop-down menu to determine the menu action button—for example, **Graphics** or **Alarms**—to be active when SiteScan Web starts.

Change Preferences

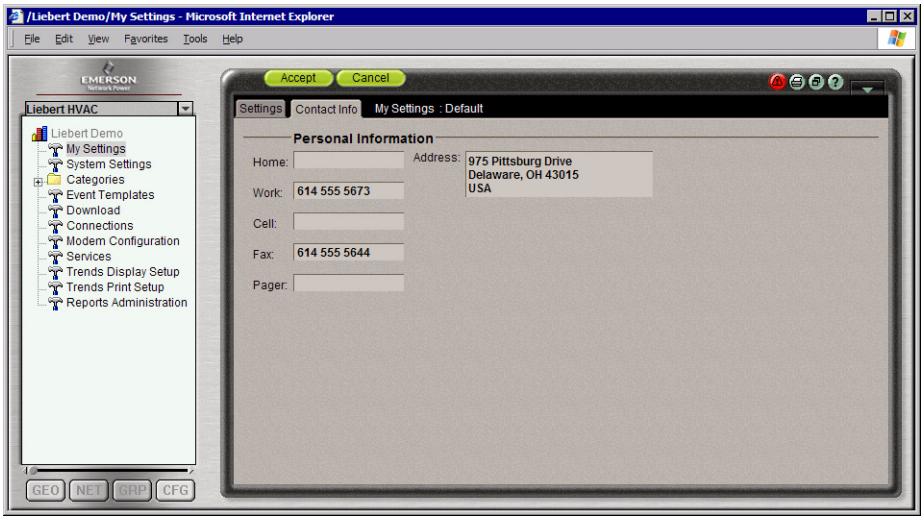
- The Language box has a drop-down menu of available languages. To set up your system for a language other than English, see the Help file for detailed procedures.
- Click to place a check mark (✔) in the **Automatically collapse trees** box to expand only one tree branch at a time.
- Click to place a check mark (✔) in the **View commissioning tools** box to access commissioning tools and their related reports.
- You may specify a custom sound file (with the extension **.au** or **.wav**) for each alarm type. Click to place a check mark (✔) in the alarm type box—**Non-critical alarms** or **Critical alarms**—and enter the file name with its path in the corresponding Sound File text box.

Save Changes

- When finished, click **Accept** (or **Cancel** to close the window without saving your changes).

12.1.2 Contact info

- Click on the **CFG** button, then click on **My Settings** in the tree at left.
- Click on the **Contact Info** tab to display the following window.



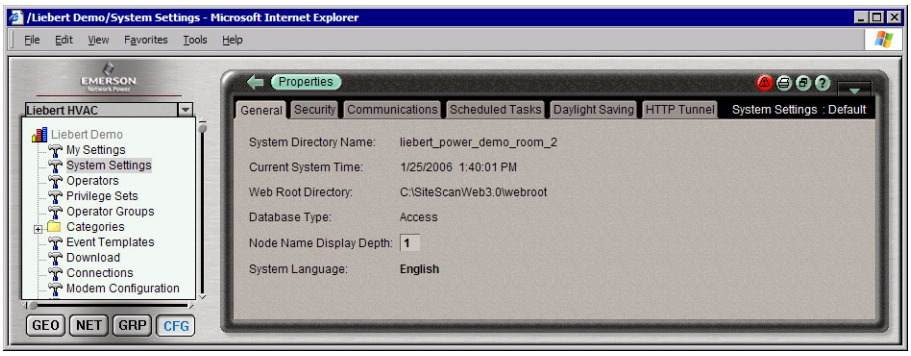
- Enter your contact information in the text boxes:
  - Enter telephone numbers for **Home**, **Work**, **Cell**, **Fax** and **Pager**.
  - Enter your work location in the **Address** box.
- When finished, click **Accept** (or **Cancel** to close the window without saving your changes).

12.2 System Settings

This section describes two tabs in System Settings: **General** and **Daylight Saving**.

12.2.1 General

- Click on the **CFG** button, then click on **System Settings** in the tree at left.
- Click on the **General** tab to display the following window.

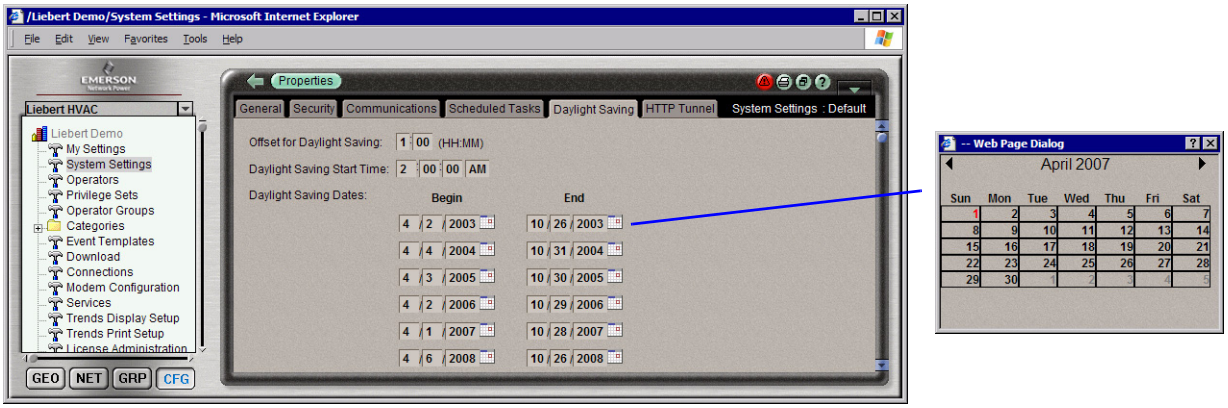


- The **General** tab displays the following system information (not editable):
  - System Directory Name
  - Current System Time
  - Path to the Web Root Directory
  - Database Type
  - System Language
- The Node Name Display Depth box shows the number of levels displayed in paths in SiteScan Web. For example, if this value is set at:
  - 2, a typical path might be ..\AHU\RA Temp
  - 3, a typical path might be ..\Atlanta R&D\First Floor\AHU

  Changing this field does not take effect until you restart SiteScan Web Server.

12.2.2 Daylight Saving

- Click on the **CFG** button, then click on Daylight Saving in the tree at left.
- Click on the **General** tab to display the following window.



- The Offset for Daylight Saving time should be 1 hour. Enter using the format HH:MM (01:00).
- The Daylight Saving Start Time is typically 2:00 a.m. Enter in the format HH:MM:SS (02:00:00), then click on the AM/PM box to toggle between **AM** and **PM**.
- The Daylight Saving Dates should be filled in with a Begin and End date for each year. To make a change, enter the date in the format MM/DD/YYYY or click on the calendar icon and click on the desired date in the calendar that opens.

12.3 Set Up Users

The Administrator may set up users, defined as *Operators* in SiteScan Web, with customized access privileges. These operators may also be designated as recipients of alarm messages, as described in **9.4 - Actions**.

NOTES

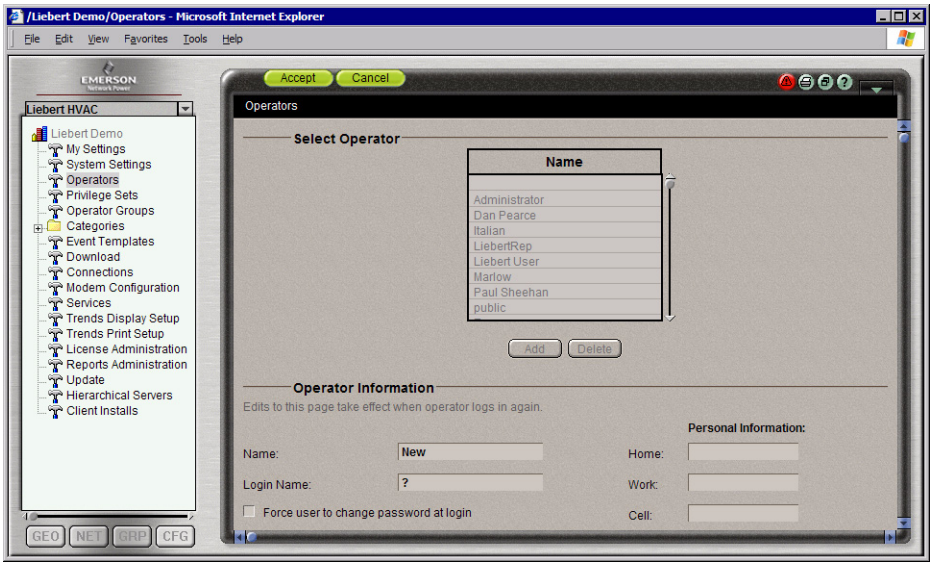
SiteScan Web comes with a default ***Administrator*** *operator. For security, either assign a password to this operator or delete it after assigning Admin privileges to another operator.*

With hierarchical servers, you must create identical operators on each server.

Users may be assigned to *Operator Groups* to simplify the process of assigning access privileges and setting up recipients for alarm messages, as described in **12.3.2 - Create Operator Groups**.

12.3.1 Set Up Operators

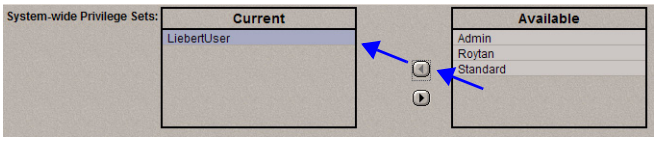
- Click on the **CFG** button, then click on **Operators** in the tree at left.



- Click the **Add** button to create a new user. The new operator's data appears below the button. Use the scroll bar to view the lower portions of the window.

  The window is divided into these sections (some fields are the same as in **12.1 - My Settings**):
- In the **Operator Information** section:
  - In the Name box, enter a name as you want it to appear on lists in SiteScan Web menus.
  - In the Login Name box, enter a name for the operator to enter when logging in. This name must be unique within the system.
  - To prompt operators to create their own passwords, click to place a check mark (✔) in the **Force user to change password at login** box. Be sure to assign a temporary password.
  - Complete the remaining fields, which are described in **12.1 - My Settings**, for this operator.
- The **Groups** section appears only if you have created at least one Operator Group. To add this operator to a group, click on a group in the Available list, then click the left arrow.
- In **System-Wide Privilege Sets**, shown at right, click on any group in the Available list, then click the left arrow to assign that privilege set to the Current operator.

  To remove an item from the Current list, select it and click the right arrow.



  Note: The Current list shows all privilege sets assigned to this operator. A grayed-out privilege set indicates it was assigned to the operator through the operator group shown in parentheses.
- In the **UI Settings** section, make changes as needed for this operator (all fields in this section are the same as in **12.1 - My Settings**).
- When finished, click **Accept** (or **Cancel** to close the window without saving your changes).

12.3.2 Create Operator Groups

Users may be assigned to *Operator Groups* to simplify the process of assigning access privileges and setting up recipients for alarm messages. This step requires that individual operators have been created, as described in **12.3.1 - Set Up Operators**.

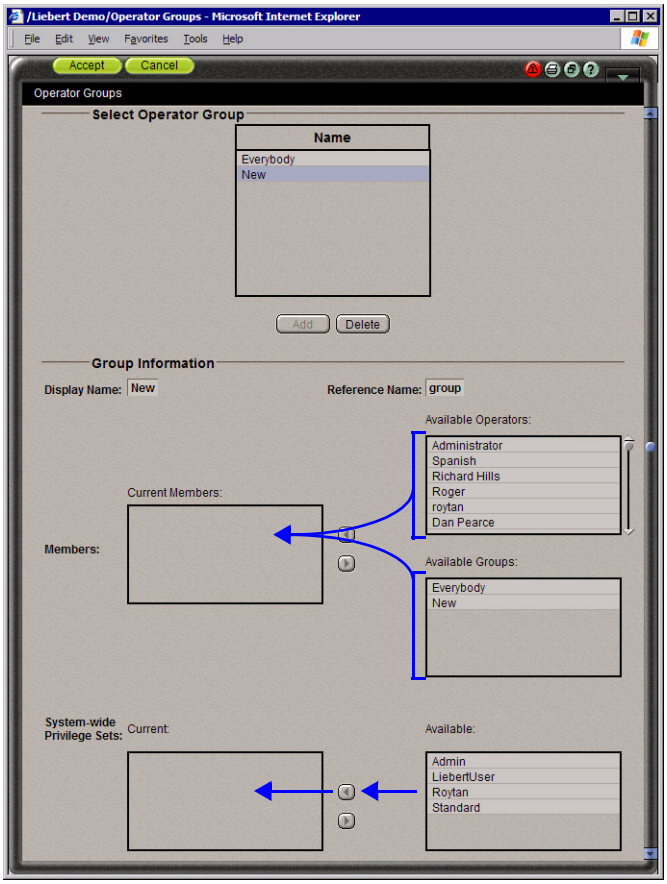
NOTE

*SiteScan Web comes with a permanent default group called **Everybody** that automatically includes all operators as members. You may assign privilege sets to this default group.*

- Click on the **CFG** button, then click on **Operator Groups** in the tree at left.
- Click the **Add** button to create a new group. The new group's data appears below the button. Use the scroll bar to view the lower portions of the window.
- In the Display Name box, enter a name as you want it to appear on lists in SiteScan Web menus.
- In the **Members** section, you may add existing individual operators or another group to the new group. Members must be added one at a time.

  To do this:
  - Click on a name in the Available Operators or Available Groups list.
  - Click on the left arrow to move that name to the Current Members box.
  - Repeat the process as needed until all members of the group appear in the Current Members box.
  - To remove a member from the group, click on the name in the Current Members box, then click on the right arrow.
- In **System-Wide Privilege Sets**, you may add existing privilege sets to the new group.

  To do this:
  - Click on any group in the Available list, then click the left arrow to assign that privilege set to the Current group.
  - To remove an item from the Current list, select it and click the right arrow.
- When finished, click **Accept** (or **Cancel** to close the window without saving your changes).



12.4 Assign Privileges to Users

You may create *Privilege Sets*—permission to use selected features in SiteScan Web—and assign them to individual operators and operator groups.

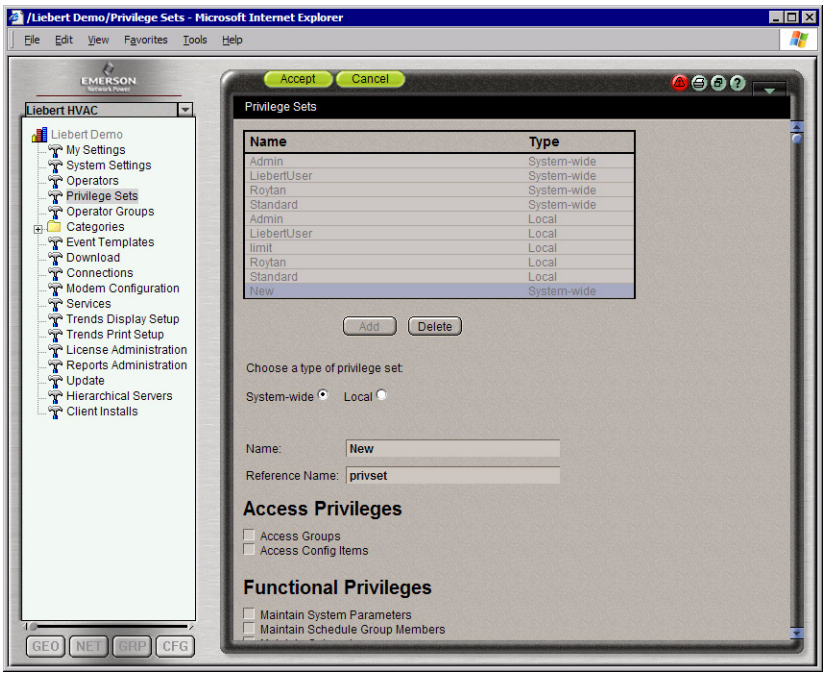
NOTE

*SiteScan Web comes with a default privilege set called **Admin** that includes most privileges. Only an operator with the Admin privilege set can perform the following functions that are not controlled by privileges:*

- *Add, edit or delete operators, operator groups and privilege sets.*
- *Update SiteScan Web Server.*
- *Register the SiteScan Web license.*
- *Enable and set up advanced security features such as location-dependent operator access and a configurable password policy (if included in your system).*

12.4.1 Add a Privilege Set

- Click on the **CFG** button, then click on **Privilege Sets** in the tree at left.



- Click the **Add** button to create a new set of privileges. The new privilege set's data appears below the button. Use the scroll bar to view the lower portions of the window.
- Click on a radio button to choose the type of privilege set: **System-wide** or **Local**. Each option brings up a corresponding list of privileges.
- In the Display Name box, enter a name for the privilege set as you want it to appear on lists in SiteScan Web menus.
- Click to place a check mark (✔) for each privilege you want to include in this privilege set. Refer to **Table 8** for a complete list with descriptions.
- When finished, click **Accept** (or **Cancel** to close the window without saving your changes).

Table 8 provides descriptions for all privileges available in the **Privilege Sets** window.

Table 8 Privilege descriptions

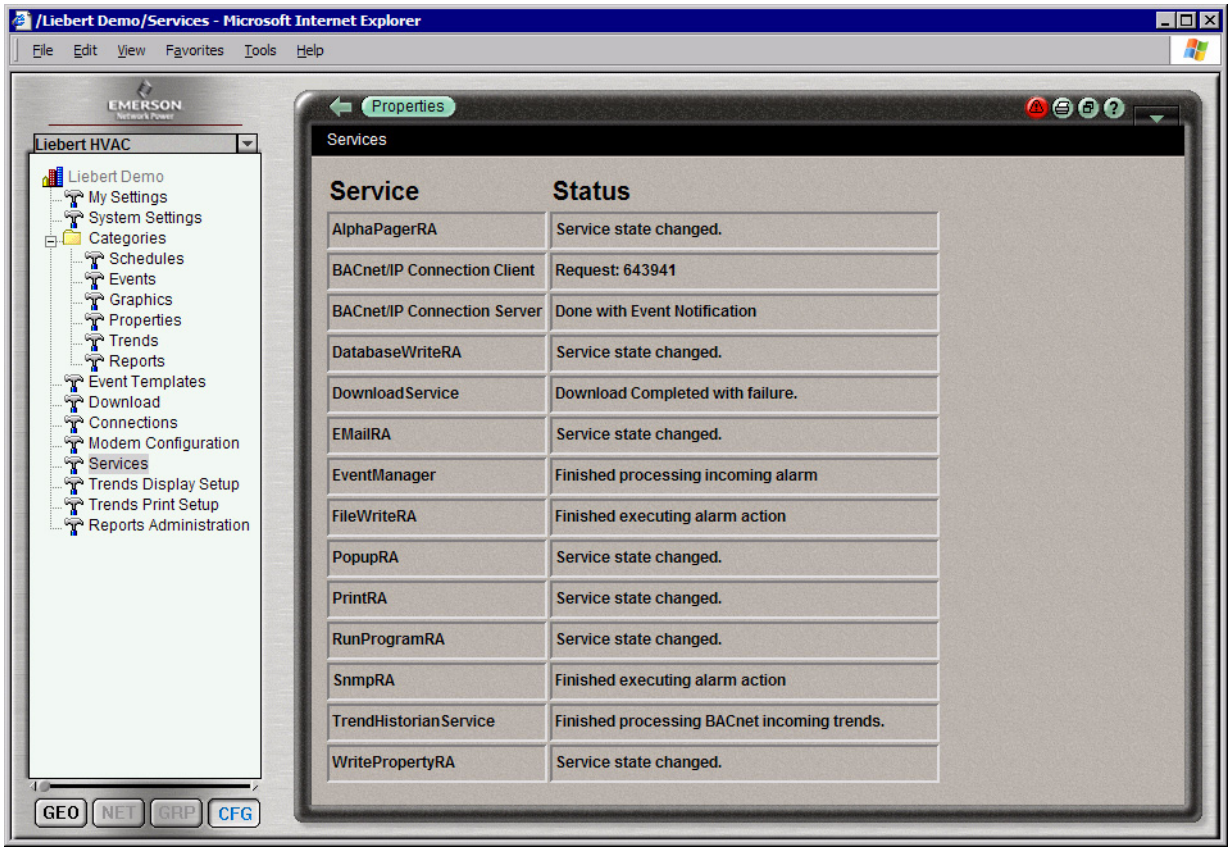
Access Privileges	Permits Operators to Access But Not Edit...
Access Geographic Locations	pages from the GEO tree.
Access Network Items	pages from the NET tree.
Access Groups	pages from the GRP tree.
Access Config Items	pages from the CFG tree.
Access Alarms	alarms.
Access User Category 1-5	anything in a category that has the same privilege assigned to it.
Parameter Privileges	**Permits Operators to Edit Properties such as...**
Edit Setpoint Parameters	occupied and unoccupied heating and cooling setpoints.
Edit Tuning and Logic Parameters	gains, limits, trip points, hysteresis, color bandwidths, design temperatures, and optimal start/stop.
Edit Manual Override Parameters	locks on input, output, and network points.
Edit Point Setup Parameters	point number, type, range, and network source and destination.
Edit Restricted Parameters	properties the installer restricted with this privilege.
Edit Category Assignments	Alarm, Graphic, Trend, and Report category assignments.
Edit History Value Reset	elapsed active time and history resets, and runtime hours.
Edit Trend Parameters	enable trend logging, log intervals, and log start/stop times.
Edit Calibration Parameters	point calibration offsets.
Edit Hardware Device Parameters	module driver properties.
Edit Critical Configuration	critical properties the installer protected with this privilege.
Edit Area Name	area display names.
Edit Equipment Name	equipment display names.
InterOp Privilege 1 - 10	those protected by password levels 1-10 in SuperVision.
Functional Privileges	**Permits Operators to...**
Manage Alarm Messages and Actions	add, edit, and delete alarm messages and actions.
Maintain System Parameters	edit all properties on the System Settings page.
Maintain Schedules	add, edit, delete, and download schedules.
Maintain Schedule Group Members	add, edit, and delete schedule groups.
Maintain Categories	add, edit, and delete categories.
Maintain Trends Display and Print Setup	edit Trends Display Setup and Trends Print Setup on the CFG tree.
Maintain Alarm Templates	edit Alarm Template and Reporting Action Templates.
Acknowledge Non-Critical Alarms	acknowledge all non-critical alarms.
Acknowledge Critical Alarms	acknowledge all critical alarms.
Force Normal Non-Critical Alarms	force non-critical alarms to return to normal.
Force Normal Critical Alarms	force critical alarms to return to normal.
Delete Non-Critical Alarms	delete non-critical alarms.
Delete Critical Alarms	delete critical alarms.
Download Devices	mark equipment for download and initiate a download.
System Shutdown	issue the Shutdown manual command that shuts down SiteScan Web Server.
Engineer System	log in and make database changes in SiteBuilder; use the copy, notify, reload, and revert manual commands; edit the reference names and display names of equipment from a SiteScan Web browser.
Maintain Graphs and Reports	add, edit, and delete trend graphs and reports.
Maintain Connections	edit Connections page properties.
Remote File Management	access files using a WebDAV utility.
Remote Data Access	retrieve SiteScan Web data through an Enterprise Data Exchange (SOAP) application.
Manual Commands/Console Operations	access the manual command dialog box and issue basic manual commands.
Manual Commands/File IO	execute manual commands that access the server's file system.
Manual Commands/Adv Network	execute manual commands that directly access network communications.
Manual Commands/Unrestricted	execute manual commands that bypass all safeguards and may cause unpredictable results if used incorrectly.

12.5 Services

The Services window displays all current services for SiteScan Web and the current status of each.

To access the Services window:

- Click on the **CFG** button, then click on **Services** in the tree at left.

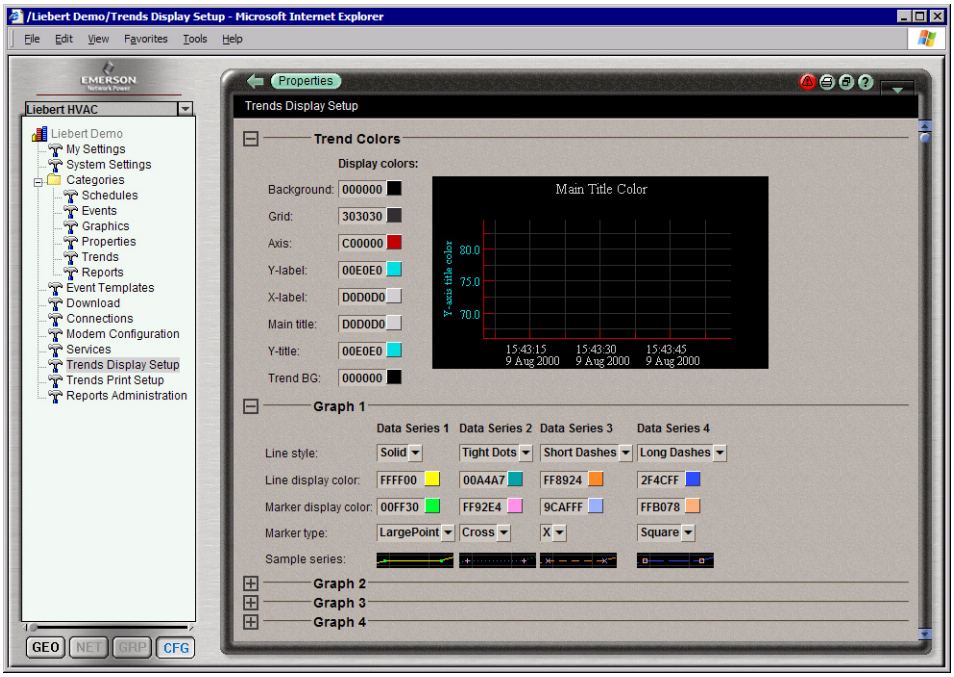


12.6 Trends Setup

12.6.1 Trends Display Setup

The Trends Display Setup options allow you to specify the appearance of graphs on the screen.

- Click on the **CFG** button, then click on **Trend Display Setup** in the tree at left.

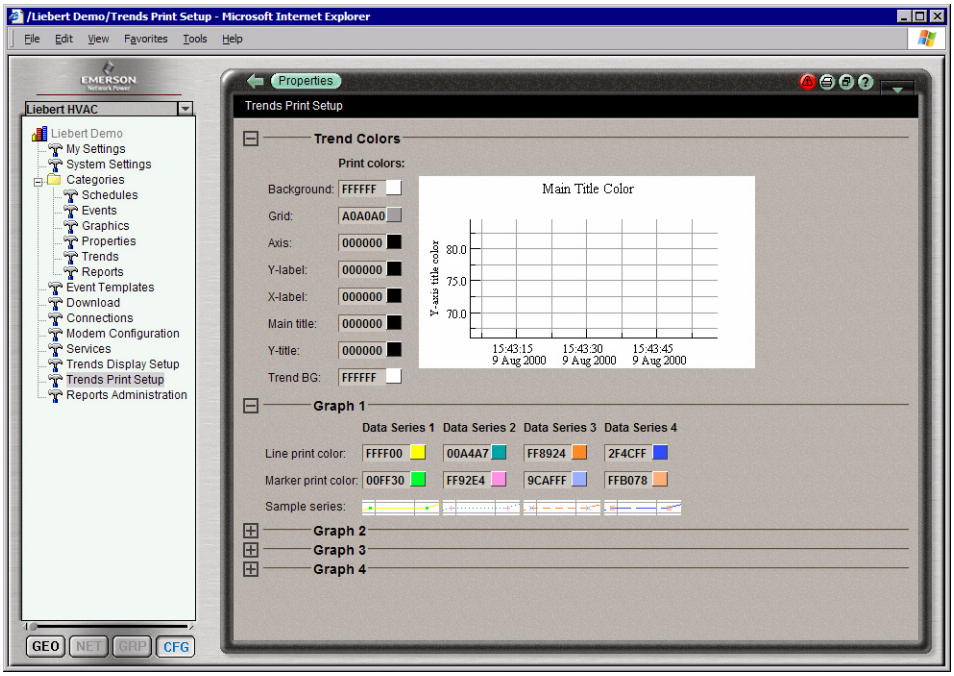


- In the Trend Colors section, choose options to specify colors for all graphs for the background, grid and axis, as well as text portions: labels for x-axis and y-axis labels, the main title and the y-axis title.
- You may set up display options for up to four types of graphs, including line style and color and marker color and type.

12.6.2 Trends Print Setup

The Trends Print Setup options allow you to specify the appearance of graphs on the printer.

- Click on the **CFG** button, then click on **Trends Print Setup** in the tree at left.



- In the Trend Colors section, choose options to specify colors for all graphs for the background, grid and axis, as well as text portions: labels for x-axis and y-axis labels, the main title and the y-axis title.
- You may set up display options for up to four types of graphs, including line style and color and marker color and type.

12.7 Client Installs

Client Install is used to install the Java Virtual Machine on the current connected workstation. Install only if required.

Wafer Font is used by SiteScan Web to display specific text in the SiteScan Web session. Install only if required.

Alarm Pop Application is a thin application that can be used by a client to receive alarm notifications to a workstation outside of the SiteScan Web browser.

Click a link to download:

- Sun's Java VM: Java Virtual Machine plugin for Internet Explorer applets.
- Wafer font: Wafer font for use with logic pages. (Place in your Windows install directory/fonts folder.)
- Alarm Popup Application: Stand-alone client application that receives Alarm Popup action messages.

13.0 LIEBERT SOFTWARE PROGRAM LICENSE AGREEMENT

This section contains the license agreement for SiteScan Web.

LIEBERT SITESCAN WEB SOFTWARE LICENSE AGREEMENT

Liebert Corporation
End User License Agreement (EULA)

This End User License Agreement (EULA) is a CONTRACT between the User, and Liebert Corporation (Liebert), which covers the User's use of the Liebert products (Products) that accompany this EULA, which may include software programs (Software), hardware (Hardware), associated media, printed materials, and "online" or electronic documentation. If the User does not agree to the terms of this EULA, then do not install or use the Software Product or the License. BY EXPLICITLY ACCEPTING THIS EULA, HOWEVER, OR BY INSTALLING, COPYING, DOWNLOADING, ACCESSING, OR OTHERWISE USING THE SOFTWARE PRODUCT AND/OR LICENSE, YOU ARE ACKNOWLEDGING AND AGREEING TO BE BOUND BY THE TERMS OF THIS EULA.

COPYRIGHT

Copyright laws and international copyright treaties, as well as other intellectual property laws and treaties protect the Products. User may not and shall not copy or otherwise reproduce or make available to any other party any part or all of the Products. The User may, however, make one (1) copy of Software for backup or archival purposes.

DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS

User may not reverse engineer, decompile or disassemble the Products, modify or create derivative works based upon the Products in whole or in part, distribute copies of the Software, remove any proprietary notices or labels on the Products or resell, lease, rent, transfer, sublicense or otherwise transfer rights to the Software. User acknowledges that no title to the intellectual property in the Products is transferred. Title, ownership, rights and the intellectual property rights in and to the Products shall remain with Liebert. Furthermore, this EULA does not grant User any rights in connection with any trademarks or service marks of Liebert.

GRANT OF NON-EXCLUSIVE LICENSE

Liebert Software that does not require registration (typically engineering tool software programs and training software programs) may be installed and used on multiple computers within the User's organization as required, but may not be shared with individuals outside the User's organization. User may not modify or create derivative copies of the License. User may not sublicense, reassign, or transfer this License or Agreement, or any part thereof, to any party. All rights not expressly granted to User are retained by Liebert.

WARRANTIES

Licensor warrants that Licensor has the right to license to User the nonexclusive use of the Products as set forth herein. Licensor warrants that, to the best of Licensor’s knowledge, the intellectual property embodied in the Products do not infringe upon the registered U.S. copyright, patent, or trademark rights of third parties. ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE ARE HEREBY EXCLUDED.

INDEMNIFICATION

In the event of any United States copyright, patent, or trademark infringement claim brought against User arising out of use of the Product as authorized in this EULA, Licensor will defend, at its expense, and pay any direct costs and damages made in settlement or finally awarded as a result of any infringement action brought against User, subject to the limitations set out in the next paragraph, provided (1) Licensor is promptly notified in writing by User that such action is threatened or has been brought; (2) Licensor shall have sole control of the defense of any such action and all negotiations for its settlement or compromise; and (3) Licensor receives the cooperation and assistance of User.

(continued)

LIEBERT SITESCAN WEB SOFTWARE LICENSE AGREEMENT *(continued)*

LIMITATION ON LIABILITY

Licensor shall not be liable for loss of profit, loss of business, or other financial loss which may be caused, directly or indirectly, by the inadequacy of the Product for any purpose or any use thereof, or by any defect or deficiency therein. The User agrees that the Licensor's liability for damages, if any, shall not exceed the charges paid to the Licensor by the User under this Agreement. No action, regardless of form, arising out of any transaction under this Agreement may be brought by the User more than one year after the Licensee has knowledge of the occurrence which gives rise to the cause of such action.

ADDITIONAL SOFTWARE

This EULA applies to updates or supplements to the original Product provided by Liebert.

TERMINATION

Liebert may cancel this EULA if User does not abide by the terms and conditions of this EULA, in which case all Products and component parts must be returned to Liebert and all copies of Products, or any portions thereof, not returned to Liebert, must be destroyed.

NOTE ON JAVA SUPPORT.

Sun Microsystems, Inc. has contractually obligated Liebert to make this disclaimer:

THE PRODUCT MAY CONTAIN SUPPORT FOR PROGRAMS WRITTEN IN JAVA. JAVA TECHNOLOGY IS NOT FAULT TOLERANT AND IS NOT DESIGNED, MANUFACTURED, OR INTENDED FOR USE OR RESALE AS ONLINE CONTROL EQUIPMENT IN HAZARDOUS ENVIRONMENTS REQUIRING FAIL-SAFE PERFORMANCE, SUCH AS IN THE OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION OR COMMUNICATION SYSTEMS, AIR TRAFFIC CONTROL, DIRECT LIFE SUPPORT MACHINES, OR WEAPONS SYSTEMS, IN WHICH THE FAILURE OF JAVA TECHNOLOGY COULD LEAD DIRECTLY TO DEATH, PERSONAL INJURY, OR SEVERE PHYSICAL OR ENVIRONMENTAL DAMAGE ENTIRE AGREEMENT.

This EULA, including any addendum or amendment to this EULA which is included with the Product, are the entire agreement between User and Liebert relating to the Products, and they supersede all prior or contemporaneous oral or written communications, proposals and representations with respect to the Products or any other subject matter covered by this EULA. To the extent the terms of any Liebert policies or programs for support services conflict with the terms of this EULA, the terms of this EULA shall control.

CONTACT INFORMATION

If the User has any questions about this EULA, or wants to contact Liebert for any reason, please direct all correspondence to: Liebert Corporation, Attn: Marketing Department, 975 Pittsburg Drive, Delaware, OH 43015, United States of America.

© 2003 Liebert Corporation

The Company Behind the Products

With over a million installations around the globe, Liebert is the world leader in computer protection systems. Since its founding in 1965, Liebert has developed a complete range of support and protection systems for sensitive electronics:

- Environmental systems—close-control air conditioning from 1 to 60 tons
- Power conditioning and UPS with power ranges from 300 VA to more than 1000 kVA
- Integrated systems that provide both environmental and power protection in a single, flexible package
- Monitoring and control—from systems of any size or location, on-site or remote
- Service and support through more than 100 service centers around the world and a 24/7 Customer Response Center

While every precaution has been taken to ensure the accuracy and completeness of this literature, Liebert Corporation assumes no responsibility and disclaims all liability for damages resulting from use of this information or for any errors or omissions.

© 2006 Liebert Corporation
All rights reserved throughout the world. Specifications subject to change without notice.

® Liebert and the Liebert logo are registered trademarks of Liebert Corporation. All names referred to are trademarks or registered trademarks of their respective owners.

SL-27050 (2/06) Rev. 1

Technical Support / Service

Web Site
www.liebert.com

Monitoring
800-222-5877
monitoring@liebert.com
Outside the US: 614-841-6755

Single-Phase UPS
800-222-5877
upstech@liebert.com
Outside the US: 614-841-6755

Three-Phase UPS
800-543-2378
powertech@liebert.com

Environmental Systems
800-543-2778

Outside the United States
614-888-0246

Locations

United States
1050 Dearborn Drive
P.O. Box 29186
Columbus, OH 43229

Europe
Via Leonardo Da Vinci 8
Zona Industriale Tognana
35028 Piove Di Sacco (PD) Italy
+39 049 9719 111
Fax: +39 049 5841 257

Asia
7/F, Dah Sing Financial Centre
108 Gloucester Road, Wanchai
Hong Kong
852 25722201
Fax: 852 28029250

Emerson Network Power.
The global leader in enabling Business-Critical Continuity.

EmersonNetworkPower.com

- AC Power Systems
- Connectivity
- DC Power Systems
- Embedded Power
- Power Protection
- Integrated Cabinet Solutions
- Outside Plant
- Precision Cooling
- Site Monitoring and Services

Emerson Network Power and the Emerson Network Power logo are trademarks and service marks of Emerson Electric Co. ©2005 Emerson Electric Co.